Las redes sociales atlantistas como instrumentos de soft power y hard power en el contexto de la ciberguerra

Por: Jorge Alberto Lizama Mendoza
Globalizacion, 14 de octubre 2018

Región: EEUU
Tema: Guerra

Introducción

Hoy en día se asiste a un escenario que marca un cruce entre dos ámbitos que regularmente se asumen como lejanos; por un lado, la ciberguerra y su modelo C4ISR, el cual se integra por los elementos de control, comando, comunicación, computadoras, inteligencia, vigilancia y reconocimiento. Por otra parte, las redes sociales atlantistas que dominan internet (Google, Apple, Facebook, Amazon, Twitter, Microsoft), mismas que promueven los intereses imperialistas de los Estados Unidos y la OTAN.

En el cruce, las redes sociales atlantistas ya no son sólo brazos de apoyo en el escenario tradicional de la ciberguerra que tiene que ver con la dimensión del *soft power*, o guerra de la información y la propaganda; también, ya han ingresado al terreno del *hard power* y han comenzado a tener impacto en el escenario de las telecomunicaciones, las armas digitales y los ejércitos de combate.

Sugerido lo anterior, se puede definir la ciberguerra como:

"El recurso de apelar a las capacidades cibernéticas para dirigir operaciones agresivas a través del ciberespacio contra objetivos militares, contra un Estado o contra su sociedad en general. También se puede definir como una "guerra clásica" en donde al menos uno de los componentes de ejecución o instrumentalización (armas, en el sentido más amplio) se basa en el campo de lo digital. (Ventre, 2011, p. 2)"

A este escenario general hay que sumar los elementos finos y constitutivos de la ciberguerra, en este sentido, uno de los modelos más influyentes hoy en día es justo de naturaleza atlantista, el llamado C4ISR que fue desarrollado desde los años 70s por los países miembros de la OTAN y que ha logrado una gran eficacia teórico/práctica al sumar elementos propios de la tecnología digital.

Así pues, el C4ISR es un sistema militar de acción basado en los elementos de:

"Comando, Control, Comunicaciones, Computadoras, Inteligencia, Vigilancia y Reconocimiento (...) El sistema C4ISR es un sistema de sistemas y también puede denominarse red de redes ya que funciona sobre principios similares a los de Internet (Zubairi y Mahoboob (2012), p. 224)"

Figura 1: Elementos del Modelo C4ISR de la ciberguerra

A continuación, se explica el impacto de las redes sociales atlantistas en el modelo C4ISR.

NIVEL 1: INTELIGENCIA, VIGILANCIA Y RECONOCIMIENTO

En este nivel, las acciones están encaminadas a estudiar la capacidad del oponente y sus puntos débiles a nivel de infraestructuras físicas e informativas; también se encarga de analizar el perfil de sus habitantes y las formas propagandísticas en que se les puede predisponer para que promuevan determinados escenarios, o para dirigirlos a un punto muerto (destruir el ánimo de combate).

En las redes sociales atlantistas, el núcleo de apoyo al nivel 1 se soporta a través de la asociación entre BIG DATA + BIG BROTHER. El primero trabajando en los escenarios públicos y globales de la información (economía, política o población); el segundo, centrando en la esfera privada de la información y el usuario.

1. a) Big data (apoyo al elemento de la inteligencia)

Para el rubro particular de la inteligencia, el atlantismo ha encontrado en el big data, la fórmula más idónea para comenzar a analizar y entender el funcionamiento de una nación o región contraria a sus intereses. El big data es un conjunto de datos cuyo volumen, procesamiento y velocidad de respuesta supera a las bases de datos tradicionales, teniendo que utilizar miles de redes de almacenamiento de información que trabajan en conjunto.

Google-Alphabet, la mayor corporación de manejo de datos a nivel mundial, tiene el papel histórico de ser la piedra inicial de un proceso progresivo de big data que inició en 1998 bajo la fórmula de un simple buscador y que hoy en día, tras la compra de más de 100 compañías relacionadas con el campo de la tecnología digital (Blogger, Youtube, Picasa o Ad Word, entre otras), se ha convertido en el más importante centro de big data de de la historia.

Google controla información sensible para el campo de la inteligencia militar, por ejemplo, con sus adquisiciones ya controla:

- Los mapas geográficos (Google Earth)
- Las rutas y tiempos concretos entre destinos geográficos (Google Maps)
- Cómo lucen avenidas y calles (Google Street)
- El monitorear vía satelital y en tiempo real minas, presas, cultivos agrícolas (Google Skybox)
- El monitorer la atmósfera en tiempo real (Titan Aerospace)
- El monopolio en el acceso a la información en internet (Google buscador)
- El monopolio de la información en video en internet (Youtube)
- El monopolio de correos electrónicos (Gmail)
- El monopolio, control y ubicación en tiempo real de la mayor parte de teléfonos celulares (Google Apps)
- La creación de robots militares pare el ejército de los Estados Unidos (Boston Dynamics)

Si se suman los escenarios diversos de información que Google logra obtener a través de sus servicios, se tiene no sólo una ecología informativa de alcance a nivel mundial, sino también los insumos ilimitados para que a través del big data se puedan situar en poco tiempo los patrones de fortaleza y/o debilidad de una nación o región. No es de extrañarse que uno de sus fundadores, Erick Schmidt, quien fue del a 2002 al 2011 director ejecutivo de la empresa, ahora tenga un cargo como jefe del Consejo de Innovación en el Ministerio

de Defensa de los Estados Unidos, es decir, el Pentágono.

1. b) Big Brother (apoyo a los elementos de la vigilancia y el reconocimiento)

El segundo elemento que soporta y se interrelaciona de manera directa con el big data es el llamado big brother.

Si durante el paradigma industrial la vigilancia se entendía mayormente como una figura de surveillance (vigilar desde arriba), donde satélites, torres de telecomunicaciones, cámaras urbanas, etc. hacían la labor de vigilar a los controlados a cambio de un costo muy elevado para gobiernos y empresas. Ahora, estudioso del tema proponen que en la revolución digital se ha sumado también la sousveillance (vigilar desde abajo), un modelo inédito de "control sin lágrimas" donde la ecuación se ha invertido: ahora es el ciudadano mismo el que desea ingresar a las redes sociales atlantistas para intercambiar su información privada por las recompensas simbólicas que ofrece el soft power: likes, tuits, seguidores.

Si Google es el brazo relacional del big data, Facebook es a su vez el brazo relacional del big brother: la empresa que dirige Mark Zuckerberg, impulsada en sus orígenes por el capital de riesgo de I-Q-Tel, una empresa de la CIA, ya ha comprado más de 45 empresas de servicios digitales, entre las que sobresalen Whatsapp e Instagram.

El big brother de Facebook se articula de forma mucho más centralizada si se le compara con la cantidad de servicios que ofrece Google:

- De acuerdo con el portal *Statista*, a mediados del año 2017 su red social alcanzó los 2 mil millones de usuarios, los cuales han dejado en la plataforma sus datos personales, lo que les gusta o no les gusta, las noticias que han consultado desde la plataforma, etc.
- Asimismo, a través del impulso constante de la "moda-selfie", a partir del año 2013 Facebook ha logrado almacenar por día cerca de 350 millones de nuevas fotos al menos sus usuarios, los amigos de los usuarios, sus compañeros de trabajo, etc.
- A la recopilación de fotos de usuarios hay que agregar el hecho que una de las empresas menos conocidas de Facebook, Deep Face, tiene la patente no sólo para el reconocimiento facial, sino también para ubicar expresiones y emociones.
- A esto, todavía falta sumarle el volumen de datos privados que de manera cruzada arrojan Whatsapp e Instagram.

La mesa directiva de Facebook también integra personalidades aliadas a los intereses financieros del atlantismo: Howard Cox (que forma parte de la mesa directiva de In-Q-Tel), Jim Breyer (que forma parte de la mesa directiva de Walmart) o Peter Thiel (fundador y CEO de Paypal).

NIVEL 2: COMUNICACIONES Y COMPUTADORAS

La función del nivel 2 en el C4ISR no sólo es mantener las comunicaciones entre los elementos que forman parte del sistema de la ciberguerra, sino también prospectar y anular las posibilidades de respuesta y reacomodo real del enemigo. Relacionado al escenario dela tecnología digital, este nivel engloba a las infraestructuras internacionales de datos digitales (comunicación), así como a las tecnologías destinadas a consultar la información ya

gestionada (computadoras).

Usualmente, se suele asumir que las redes sociales atlantistas operan en la capa de superficie de internet, teniendo poco que ver con el apartado de la infraestructura; sin embargo, con el paso de los años tanto Google como Facebook, principalmente, han ido adquiriendo un papel decisor en los flujos internacionales de comunicación.

De acuerdo con los documentos filtrados por Edward Snowden sobre el Proyecto Prism, desarrollado por la NSA, el mapa de flujo de datos a nivel mundial está comandada por los Estados Unidos y Canadá, quienes establecen un intercambio de información dominante en relación a Europa, Latinoamérica y el Caribe, así como Asia y la Zona del Pacífico.

Figura 2: Ancho de banda y flujos de información en internet, 2011

Lo anterior sugiere que ante un caso de ciberguerra los Estados Unidos podrían cerrar sus servidores raíz de internet a las otras regiones, dejándolas casi incomunicadas. Por supuesto, el "apagón" de internet no ha ocurrido tal cual en cuanto a infraestructuras, pues generaría consecuencias mayúsculas en el contexto internacional. Pero si puede ocurrir de una forma mucho más sutil: a través del "apagón" selectivo de las redes sociales, las cuales son las que mayormente dominan la información que circula por internet.

En agosto del 2013, un "apagón" de Google durante 2 minutos generó un descenso del 40% en el tráfico internacional de Internet; el año siguiente una "caída" del servidor publicitario Double Click, también de Google, generó pérdidas millonarias para sitios como Forbes, la BBC y el Wall Street Journal. Es decir, un "apagón" intencional y localizable de dicha empresa, puede provocar una interrupción sensible en la comunicación de toda una región o país. O puede no ser un "apagón", sino un flujo masivo y dirigido de "software de estado" (nivel de computadoras) a las regiones que se consideran no aliadas.

El mismo caso de control selectivo de flujos de la información puede ocurrir con Facebook, quien además ya es dueña, junto con Microsoft y Telefónica, del más nuevo cable interoceánico de fibra óptica que corre de los Estados Unidos a España, inaugurado en el 2017 (Muñoz, 2017). De manera relacional, la empresa de Mark Zuckerberg, a través de su proyecto internet.org, es pionera en el proyecto Outernet, que busca llevar gratuitamente internet satelital a todos los rincones del planeta. Con lo cual quedaría sentadas las bases para que en un futuro muy cercano, todos los flujos de comunicación digital vía satélite, estén controlados por las empresas del atlantismo.

Además de internet.org, de Facebook, forman parte del proyecto Outernet las siguientes cuatro empresas, todas de financiamiento atlantista: Loon (propiedad de Google), Qualcomm (propiedad de Virgin) y Space X (propiedad de Pay Pal).

NIVEL 3: COMANDO Y CONTROL

En el nivel tres se integran los elementos de intervención y agresión directa contra el enemigo. En la guerra tradicional este rubro está depositado en los elementos humanos y sus armas relacionales, como barcos, aviones o tanques de guerra, etc. En la ciberguerra, estos rubros se integran por los mandos estatales de ciberdefensa y sus armas relacionales: "Virus de Estado", drones, satélites espía, escopetas láser de impacto DEW (arma de energía dirigida), chatbots, bots, malware, phishing, ataques DOS, etc.

En las redes sociales atlantistas ya hay ejemplos de apoyos concretos al nivel 3: el virus Stuxnet, creado en conjunto por la inteligencia Israelí (el Mossad) y la Agencia de Seguridad Nacional de los Estados Unidos (la NSA), logró crear en enero de 2010 una pequeña fuga radioactiva en una de las instalaciones nucleares de Irán, fuga que fue corregida a tiempo, pero la cual se propagó en el Medio Oriente por las redes sociales atlantistas y el sistema operativo Windows. A Stuxnet le han seguido otros experimentos con mucha mayor capacidad destructiva como el "Proyect Sauron", bautizado por Kaspersky Lab (2016) como uno de los primeros "Virus de Estado" de la historia por su complejidad de elaboración y de ser capaz de espiar y apagar el sistema informático donde reside. Siguiendo la misma lógica, "Proyect Sauron" ha sido descubierto en sistemas informáticos de países contrarios a la OTAN, como Rusia e Irán y la amenaza ha sido "accidentalmente" propagada por las redes sociales del atlantismo.

Lo que se quiere dar a entender con lo anterior, es que esta nueva lógica de ciberguerra inaugura un modelo donde siguiendo a Vectre (2011) una mínima fuerza digital (cyber force) puede destruir sin ningún tipo de intervención/invasión física (physical force), a una infraestructura nuclear (nuclear force) y propiciar que la nación afectada acepte de inmediato las condiciones diplomáticas y económicas que se le quieren imponer (diplomatic and economic force). Lo cual es un ejemplo de cómo la frontera entre una táctica considerada poco beligerante (un virus informático difundido por las redes sociales) puede tener consecuencias de muy alta beligerancia (crisis nuclear de un país) en el mundo real.

Otra herramienta estratégica en este nivel tiene que ver con Twitter, el servicio que por su inmediatez de publicación, su potencial sincronización de noticias (trending topic) y su modelo mínimo de redacción (de 140 a 280 caracteres) promueve a nivel cognitivo una tipo de información altamente "viralizable" y superficial en cuanto a presentación y reflexión profunda de los hechos.

Un ejemplo de cómo los usuarios de redes sociales y en particular de Twitter han sido transformados de manera novedosa en batallones virtuales de presión político-social, lo han sido las llamadas "Revoluciones de Colores" y las "Primaveras Árabes" llevadas a cabo por los colectivos Canvas y Otpor, ambos financiadas por la Open Society de George Soros y quienes bajo el disfraz del hacktivismo-progre, reorientaron la discusión de las redes sociales de distintos países en fuerzas sociales de pro-democracia globalista. En aquel entonces, si un egipcio o un libio salía a la calle a protestar en contra de la injerencia atlantista en su país se encontraba con que no podía hacer mucho, pues el batallón virtual, que ya había dado paso a un batallón real, no sólo ocupaba las calles, sino que tenía todo el apoyo internacional.

Probablemente, la última gran estrategia de las redes sociales atlantistas han promocionado a través del nivel 3 del C4IRS es la promoción de lo que se conoce como "Armas de migración masiva", un término acuñado por el politólogo, Kelly M. Greenhill, para explicar cuando una fuerza internacional (Estados Unidos, UK, La OTAN, la Open Society) provoca a propósito una oleada de migración humana como medio para imponer y promocionar sus políticas internacionales.

El primer caso de "armas de migración masiva" se gestó en Alemania en el 2015 y tuvo como elemento destacado a Twitter y la manipulación del hashtag: "#RefugeesWelcome, el cual desencadenó una ola de migración de Turquía a las ciudades alemanas de Berlín y Colonia, fundamentalmente.

Figura 3: Países que promovieron el hashtag: #RefugeesWelcome en Alemania (2015)

En su momento, el estudio de 19 mil "tweets" originales relacionados con los refugiados que el investigador ruso Vladimir Shalak realizó a través del software, "Scai4Twi (enfocado a analizar los contenido de Twitter)"; arrojó que sólo el 6,4% de todos los tweets de bienvenida fueron realizados en Alemania y que más del 36% vinieron de parte de países atlantistas: Reino Unido, Estados Unidos y Australia.

Conclusiones

Si en sus inicios internet fue un proyecto planeado por la esfera militar y luego paso a ser desarrollado por la esfera académica; hoy en día vuelve a completar el círculo y regresa a servir a su amo original.

Si antes internet valoraba lo público, ahora la ciberguerra y sus redes sociales manipulan lo público con fines privados. Si antes se intentaba vincular, hoy el modelo C4ISR intenta vigilar, controlar, ideologizar, monetizar y hasta destruir al otro. Si antes la filosofía de la tecnología traía consigo la promesa del "dispositivo"; un archivo de la memoria y la cultura humana a disposición neutra de cualquiera que esté conectado. Ahora, el capitalismo de datos ha propuesto como figura eje al "servomecanismo": una "tecnología digital que sirve a sus usuarios y al mismo tiempo los pone a su "servicio".

A nivel teórico, probablemente ya ni siquiera se deba hablar de internet en un sentido ideal pues las arquitecturas privadas, panópticas y centralizadas que han impuesto las redes sociales atlantistas; son las que van a triunfar a futuro si se hace caso a sus indicadores de crecimiento y adopción. A su vez, los países que en los últimos años han experimentado los efectos de las redes sociales atlantistas, han aprendido la lección y han optado por crear también sus propias redes feudales, sus propios "jardines privados": China tiene ya su propio Facebook (Tencent), su propio Twitter (Sina Web) y su propio Amazon (Ali Express). Por su parte, Rusia también tiene su propio Facebook (VK), su Twitter (Odnoklassniki) y hasta su Whatsapp (Telegram). De acuerdo a estas tendencias, en un futuro cercano internet se disgregará en regiones geopolíticas controladas por las potencias en turno y la ciberguerra se tratará de proteger la propia infraestructura de comunicación digital a la vez que se intenta sabotear a la del enemigo.

Jorge Alberto Lizama Mendoza

Bibliografía:

Corbertt, James (9 octubre 2011) Meet In-Q-Tel, the CIA's Venture Capital Firm. *The Corbet Reportt*

Recuperado de: https://www.corbettreport.com/meet-in-q-tel-the-cias-venture-capital-firm-preview/

Cooper Smith (18 septiembre 2013) Facebook Users Are Uploading 350 Million New Photos Each Day. Business Insider. Recuperado de: http://www.businessinsider.com/facebook-350-million-photos-each-day-2013-9

Kaspersky Lab (julio 2016) *The Projectsauron APT*. GREAT.

Recuperado de https://securelist.com/files/2016/07/The-ProjectSauron-APT_research_KL.pdf

Kopfstein, Janus (12 abril 2012) *Stuxnet virus was planted by Israeli agents using USB sticks, according to new report.* The Verge. Recuperado de: https://www.theverge.com/2012/4/12/2944329/stuxnet-computer-virus-planted-israeli-agent-iran

Muñoz, Ramón (5 junio 2017) *El cable submarino de Facebook, Microsoft y Telefónica llega a España*. El País.

Recuperado de: https://elpais.com/economia/2017/06/03/actualidad/1496480418_250810.html

Oriental Review (21 septiembre 2015) *Who is twitter-luring refugees to Germany?.* Oriental Review. Open Dialogue Reserch Journal. recuperado de: https://orientalreview.org/2015/09/21/who-is-twitter-luring-refugees-to-germany/

RT (17 agosto 2013) *Los dos minutos que duró la caída de Google 'matan' el 40% del tráfico global de Internet.* Actualidad RT.

Recuperado de: https://actualidad.rt.com/actualidad/view/103153-google-caer-mundo-internet

Ventre, Daniel (Ed) (2011) *Cyberwar and information warfare*. London, UK: Wiley

FIGURAS:

Figura 1: Zubairi, Junaid y Athar Mahboob (2012) *Cyber Security Standards, Practices and Industrial Applications: Systems and Methodologies*. USA: IGI Global. P. 225

Figura 2: Eden, Grace (22 julio 2015) *Prism.* Digital Citizenship and Surveillance Society. Recuperado de: http://www.dcssproject.net/prism/

Figura 3: Oriental Review (21 septiembre 2015) *Who is twitter-luring refugees to Germany?.*