DEMOCRACIA Y BIG DATA: INCERTIDUMBRE Y DESAFÍOS CONTEMPORÁNEOS A LA GOBERNABILIDAD, LA TRANSPARENCIA Y LA DEFENSA NACIONAL

ALFREDO LEANDRO OCÓN

Magister en Estrategia y Geopolítica. Profesor titular de la materia "Nuevos Escenarios de las Relaciones Internacionales" en el Colegio Militar de la Nación (CMN) y profesor e investigador en la Escuela Superior de Guerra de Ejército (ESG). Investigador acreditado UNDEF. Co-director del proyecto "Soberanía Nacional y Ciberdefensa. Elementos teóricos y político-estratégicos del desafío ciberespacial para la Defensa Nacional", Programa de Acreditación y Financiamiento de Proyectos de Investigación "UNDEFI" de la Universidad de la Defensa Nacional (UNDEF).

Resumen

Este artículo propone abordar la problemática respecto de las redes sociales como espacio de injerencia política por parte de actores externos y como, Ponencia preparada para el XIV Congreso Nacional de Ciencia Política "La política en incertidumbre. Reordenamientos globales, realineamientos domésticos y la cuestión de la transparencia", organizado por la Sociedad Argentina de Análisis Político y la Universidad Nacional de San Martín, San Martín, 17 al 20 de julio de 2019.

ello impacta en la Defensa Nacional. Contemplando como ha sido la injerencia histórica de actores externos en cuestiones política de distintos países una serie de hechos contemporáneas ponen de manifiesto ciertas dinámicas en las Redes Sociales han dado lugar a nuevos esquemas de ejercicio de poder. A partir de dicho planteo, se indaga sobre los límites y alcances de la soberanía nacional en la actualidad, los nuevos desafíos que presenta el ciberespacio y cuáles son los dilemas estratégicos que deben afrontar, especialmente, los países periféricos.

Palabras clave:

Defensa Nacional - ciberespacio - redes sociales - geopolítica.

Abstract

This article proposes to address the problem of social networks as a space for political interference by external actors and how this impact on National Defense. Contemplating how has been the historical interference of external actors in political issues of different countries, a series of contemporary facts show certain dynamics in the Social Networks have given rise to new schemes of exercise of power. From this point of view, the present work analyzes the limits and scope of national sovereignty at present, the new challenges presented by cyberspace and what are the strategic dilemmas that must be faced, especially by peripheral countries.

Key words:

National Defense - cyberspace - social media - geopolitics.

We thought we were searching Google, but Google was searching us

Shoshana Zuboff

Introducción

Los recientes escándalos que giraron en torno a Facebook y Cambridge Analytica han puesto de manifiesto una problemática severa en cuanto la disponibilidad, el acceso y la utilización de la denominada “Big Data” en la

política. El optimismo del futuro, anclado a las nuevas tecnologías de la comunicación, las posibilidades de internet y todas las nuevas oportunidades que proporciona la llamada cuarta fase de la industrialización, se encuentra con su lado oscuro: el apogeo de un sistema de control, vigilancia y manipulación de ensueño en términos de panóptico foucaultiano.

Dicha problemática ha abierto la puerta a una serie de interrogantes que no solamente cuestionan la legitimidad de procesos políticos de gran envergadura sino también, en una escala filosófica, los límites y alcances de la libertad y la libre circulación de información, especialmente en la esfera del ciberespacio. Nos encontramos frente a la mercantilización de la información privada de los seres humanos, que pone de manifiesto una tensión: hasta qué punto la libertad en la circulación de información pone en riesgo el sistema político democrático. Es decir, el "Big Data" ofrece un nuevo recurso de poder en lo que respecta a estrategias de ingeniería social y política.

En particular, a pesar de la novedad que representa el ciberespacio y el auge recursivo del Big Data, el intento de injerencia política por medio de maniobras legales, ilegales o híbridas, ha sido una constante en la política democrática nacional e internacional. A propósito, los aportes de Dov H. Levin (2016) revelan el papel activo de las potencias, especialmente Rusia y Estados Unidos, en la actividad política local del resto de los países entre 1946 y el año 2000.

Tal como demuestra el autor (Levin, 2016) ha existido una amplia gama de estrategias de intervención o injerencia política. Sin embargo, el trabajo realizado llega hasta el año 2000, momento en que comienza a observarse el crecimiento constante de internet a escala global. La novedad es que el espacio digital y la interacción de los individuos en su interior han habilitado una nueva y poderosa herramienta para la penetración de actores externos al sistema político y una nueva reformulación de la tensión entre capitalismo y democracia.

Dicha circunstancia hace necesario apuntalar el campo de estudio de la Defensa y la Seguridad Nacional e Internacional, el papel de las nuevas tecnologías de comunicación y la intrínseca relación entre la técnica y el poder, no solamente a escala global sino también a haciendo hincapié en las diferentes formas que adquiere dichas problemáticas según el poder relativo de las naciones.

En un primer nivel, algunos interrogantes generales que se observan hoy en día son: ¿Están las instituciones de democráticas siendo socavadas por

corporaciones capaces de manipular electorados? ¿Hasta qué punto legal o ético el uso de la manipulación electoral por medio de las redes sociales? ¿Qué tipo de regulaciones e infraestructuras son necesarias para prevenir dichas capacidades? ¿Cuáles son los costos de la libre circulación de la información?

En un segundo nivel, se plantean otro tipo de interrogantes: ¿cuál ha sido el papel de actores económicos y políticos en los cambios electorales de los últimos años? ¿Cómo se diferencian las capacidades y las infraestructuras de las naciones frente a la injerencia política de actores extra-nacionales/regionales? ¿Cómo son los mecanismos de aceptación/resistencia de países periféricos?

Finalmente, en un tercer nivel, y más específicamente: ¿qué decir de las pujas entre izquierda y derecha en América Latina? ¿Hubo efectivamente participación de Cambridge Analytica en el pasado? ¿Sigue existiendo interferencia de actores extra-nacionales?

Si bien no son novedosas las reflexiones académicas en torno a dicha cuestión, aún son incipientes. Incluso, cabe destacar que gran parte de las producciones realizadas ha sido originada en centros de investigación o individuos de países desarrollados. En este sentido, existen diferencias estructurales en torno a los debates, pero también a los factores estructurales que determinan las dinámicas del fenómeno en cuestión.

Todos estos interrogantes llevan a, al menos, dos ejes de discusión anclados en la misma problemática y que obedecen a una misma necesidad estructural. En primer lugar, a los debates contemporáneos en torno al papel de las nuevas tecnologías de comunicación en la democracia y especialmente en las de países periféricos. En segundo lugar, a la capacidad de actores foráneos (estatales y no estatales) de interferir e influenciar los resultados electorales locales por medio del nuevo espacio cibernético. Ambas circunstancias obedecen, en definitiva, a una problemática estructural: la necesidad de infraestructura físicas y digitales para hacer frente a dichas cuestiones, cuestión que denota una problemática circular: la falta de infraestructura para mayor autonomía es promovida por actores que se ven beneficiados por dicha situación.

Con el fin de proponer una mirada académica a la problemática del desarrollo tecnológico asimétrico y la democracia desde los países periféricos, el presente trabajo se organiza en cuatro apartados. El primer apartado abordará, de forma descriptiva, el área de estudio que reflexiona sobre la

injerencia política de actores extra-nacionales en las dinámicas políticas locales, sobre todo considerando los aportes de Dov H. Levin (2016). En un segundo apartado, se hará un breve recorrido histórico-técnico del surgimiento y auge de internet y sus dinámicas (geo)políticas. En un tercer apartado, se profundizará sobre los orígenes técnicos de instrumentalización política de las redes sociales y su impacto actual. Finalmente, en un cuarto apartado se realizarán algunas reflexiones finales.

Intervenciones electorales: cuando las potencias tienen un voto

Tal como como lo demuestra Levin (2016), las grandes potencias despliegan con frecuencia intervenciones electorales partidistas como una importante herramienta de política exterior. Por ejemplo, los EE. UU. y la URSS/Rusia han intervenido en una de cada nueve elecciones ejecutivas competitivas a nivel nacional entre 1946 y 2000.

En este sentido, se identifican dos tipos de intervenciones. La primera es un tipo de injerencia abierta, en la cual existe una pública manifestación de apoyo o de vinculación entre el actor político o el partido local y la potencia internacional. El segundo tipo es la que se denomina intervención encubierta e implica una operación en la cual al actor político local es apoyado por una potencia forma secreta, en muchos casos involucrando maniobras ilegales o "sucias".

El argumento de Levin (2106) aspira a demostrar, por medio de análisis cuantitativo, que tales intervenciones generalmente aumentan significativamente las posibilidades electorales del candidato que recibe ayuda y que las intervenciones abiertas son más efectivas que las intervenciones encubiertas. Además, el riesgo que presenta la posibilidad del descubrimiento de la operación secreta puede implicar un importante retroceso en las aspiraciones políticas, tanto del actor poderoso involucrado como la del actor político local.

A primera vista, resulta evidente que la capacidad de observar y medir operaciones abiertas es de alguna forma más sencilla y clara que con las maniobras encubiertas, justamente por la necesidad de mantener en secreto dicho accionar. Una exitosa campaña encubierta difícilmente pueda ser rastreada, y hace de las inferencias metodológicas posibles teorías conspi-

rativas.

De forma simultánea y desde una perspectiva cualitativa, ha habido dos formas en las que ha influido en la política local. No solamente apoyando determinados tipos de actores en el juego electoral democrático, sino también en favor de cambio de régimen cuando fuera necesario. En particular, la atención en regiones tales como la latinoamericana estuvo mayormente concentrada en la dinámica de los surgimientos de gobiernos autoritarios con el apoyo directo o indirecto de los Estados Unidos.

Trabajos como los de John Nutter (2000) en "The CIA's Black Ops: Covert Action, Foreign Policy, and Democracy", colaboran con el desentrañamiento de las acciones encubiertas por parte de Estados Unidos en muchos países del mundo. La reciente desclasificación de archivos secretos no solo echa luz a muchas de estas cuestiones. Sin ir más lejos, el "Small wars manual" instaurado en 1940 para el cuerpo de Infantes de Marina, demuestra una aproximación doctrinaria a lo que denominan "pequeñas guerras":

El término "guerra pequeña" es un nombre vago para una gran variedad de operaciones militares. Aplicado a los Estados Unidos, pequeñas guerras son operaciones emprendidas, bajo autoridad ejecutiva, donde la fuerza militar se combina con presión diplomática en los asuntos internos o externos de otro Estado, cuyo gobierno es inestable, inadecuado o insatisfactorio para la preservación de la vida y de los intereses que determine la política exterior de nuestra nación. (Traducción propia SWM, 1940:1)

Hasta la caída del muro de Berlín, el accionar de la URSS no era muy diferente. Cabe destacar además que en muchos casos, como el de Chile en 1970, se pueden rastrear operaciones simultáneas por parte de las dos potencias en pugna.

El mundo post Guerra Fría y particularmente desde el atentado a las Torres Gemelas, transcurrió de forma paralela a un fenómeno en ascenso: la expansión de internet. El ascenso y la consolidación del mundo unipolar durante la década de 1990, junto al proceso de globalización creciente, encontraron sus primeros límites teóricos y empíricos en el incremento de actividades de violencia internacional que no respondían a la matriz westfaliana tradicional. A ello se sumaron lapsos de crisis económicas y sociales de alcance internacional que pusieron en jaque los preceptos y mandatos del orden internacional.

En las regiones periféricas se observó un aumento de descontento popu-

lar que se manifestó, en algunos casos, en giros a la izquierda con una impronta "anti-imperialista" y, en otros casos, en gobiernos que manifestaron abiertamente su oposición al sistema internacional.

En el caso de Medio Oriente, se observa desde 2003 un incremento en la injerencia directa e indirecta por parte de las potencias internacionales. En el continente Africano, el papel de organizaciones internacionales y el de las potencias ha colaborado con una cierta (in)estabilidad. Ahora bien, ¿qué ocurre en Latinoamérica?

Del giro a la izquierda observamos un importante avance de "la derecha" (Leiras, et al. 2016). Con dicho avance, y de forma simultánea, estalló mediáticamente un escándalo que gira alrededor de una serie de empresas de alcance internacional con la capacidad de influir en las elecciones por medio de la gestión de percepciones de los votantes a través de las redes sociales. Entre los países mencionados como posibles espacios de manipulación e interferencia electoral figuran Nigeria, Kenia, República Checa, India y la Argentina.

Lo que muchos advertían, y las desconfianzas que surgieron en torno a la rápida expansión de internet, el crecimiento de las redes sociales y la falta de controles y medidas de seguridad que acompañasen dicho proceso terminó por eclosionar en varios escándalos. Uno de los más importantes en torno a la política electoral fue el papel de una empresa llamada Cambridge Analytica y su capacidad de acceso a una de las bases de datos de individuos más grande de la historia.

¿Cómo se llegó a dicha circunstancia? Es necesario comprender cualitativamente y en un breve análisis de trayectoria cómo fue la expansión de internet y su economía política.

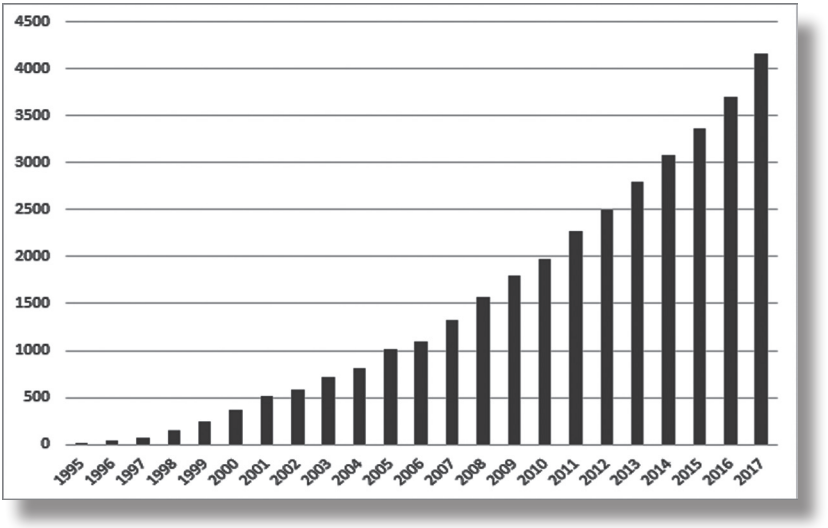
La expansión del ciberespacio

A partir de la década de 1990, la expansión de internet se tornó masiva. Una serie de hechos tanto técnicos como tecnológicos facilitó el proceso de expansión generalizada. En conjunto con una serie de cambios tecnológicos que fueron transcurriendo de forma paralela, como los avances en computadoras personales, la aparición y desarrollo de sistemas operativos como Windows, los avances en tecnología de dispositivos móviles como la comunicación en teléfonos celulares, en 1991 la World Wide Web (WWW) estuvo

disponible para el público general.

La tabla 1 muestra el crecimiento anual de usuarios con acceso a internet en el mundo entre 1995 y 2017. A primera vista, la masificación del acceso a la red tiene una explicación del tipo tecnológica: más personas con acceso a la gran red. Pero también explica un fenómeno socioeconómico y político, un proceso global de mayores interconexiones entre individuos y organizaciones.

Gráfico 1: Usuarios con acceso a internet por año (en millones de personas)



Fuente: Elaboración propia a partir de datos de *Internet WorldStats.*

Simultáneamente al proceso de expansión de internet en la población general, comenzaron a aparecer las primeras redes sociales de internet y los primeros "buscadores". Si bien podría afirmarse que los buscadores son anteriores al lanzamiento de la WWW, el papel de los buscadores cambió significativamente a partir del acceso al público general a la web.

El proceso paulatino de transformación e indexación de la web, permitió un mejoramiento en las posibilidades de los usuarios para acceder a contenidos dispersos en internet. El papel que fueron adquiriendo los buscadores, pero también las empresas detrás de su diseño y configuración, contribuyó a la configuración de nuevos actores político-económicos de la

economía global.

Los avances en las posibilidades de intercambio gracias a las redes sociales configuraron nuevas dinámicas en lo que respecta a las relaciones entre seres humanos. Paralelamente, el avance del e-commerce y del consumo de productos digitales de forma online abrió las puertas a una nueva faceta de la era de la información, marcada por el nuevo paradigma digital.

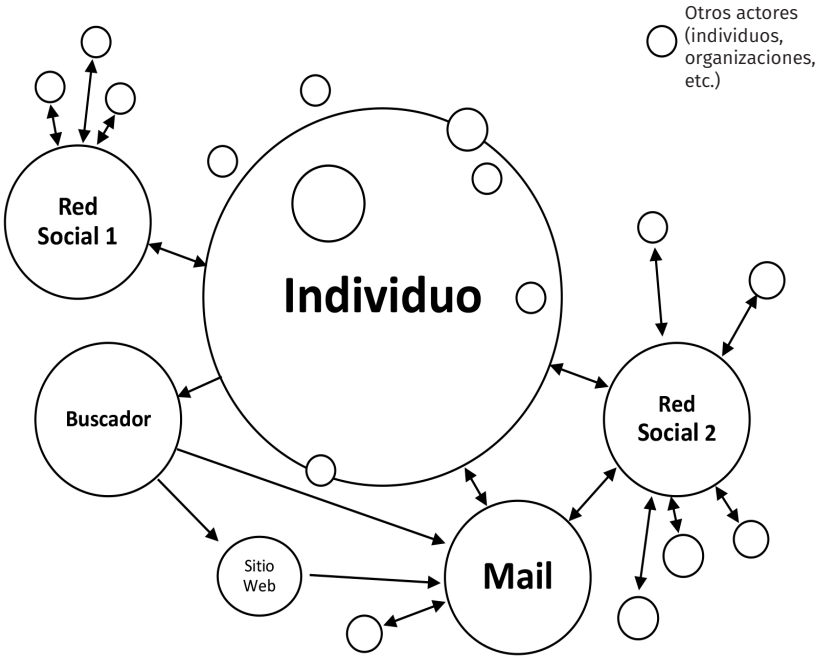
La transversalidad del ciberespacio denota una dimensión fundamental de la intervinculación de los dispositivos y la esfera digital, es decir entre lo físico y lo ciberespacial. Existen acciones que se realizan desde los dispositvos técnicos que configuran diversas dinámicas en el ciberespacio pero también, de forma inversa, existen acciones que se pueden realizar por medio del ciberespacio que afectan a los dispositivos técnicos.

Las ventajas de la interconectividad ha abierto las puertas a un gran espectro de vulnerabilidades. La mera conexión de los disposistivos a redes que pueden tener acceso a internet, por más acciones que se realicen para contrarrestar las amenazas, son un punto de vulnerabilidad. Al mismo tiempo, las ventajas obtenidas por dicha conexión aseguran en muchos casos una mejor operatividad y administración de aquello que se encuentra conectado a La Red.

En este sentido, dichos fenómenos se posicionan como puntos centrales de las (inter)relaciones en el ciberespacio. El individuo en las redes sociales accede primero a la red social, que es la aplicación o el *software.* La red se encuentra definida y es posible, por el nodo técnico que posibilita el intercambio, que todas las interacciones interindividuales se realicen por medio de la aplicación.

Por su parte, el buscador cumple el papel de un nodo transitorio. El buscador no un es nodo en el sentido estricto porque no intermedia constantemente en el intercambio del usuario con la web a la que direcciona. Sin embargo, el buscador se ha transformado en un nodo transitorio del usuario con el resto de internet. Es decir, es el mecanismo cognitivo que intermedia en la relación del usuario con las redes desconocidas por este.

Figura 5: Dinámica Nodal de las Redes Sociales, el mailing y los buscadores



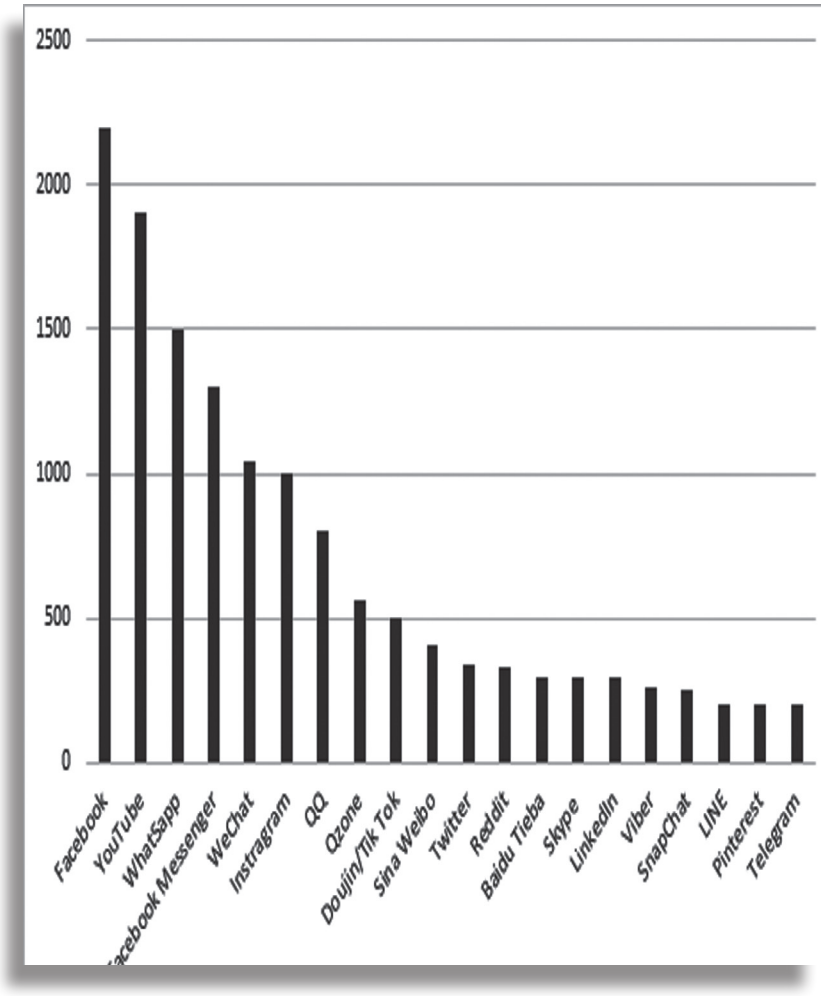
Fuente: Elaboración propia

En este sentido, la dinámica de interacción entre los individuos se encuentra nodalmente intermediada entre no solamente el servicio de internet en sí mismo, sino que su manifestación directa es el uso de una aplicación o un servicio de *mailing* que ofrece alguna empresa u organización.

En el gráfico 2, se puede observar la cantidad de usuarios activos a julio de 2018 por red social. Si bien un mismo usuario utiliza más de una red social, se pueden observar importantes diferencias entre cada una. Las primeras cinco son Facebook, YouTube, WhatsApp, Facebook Messenger[1] y WeChat.

1 Es posible una crítica a dicha categoría, debido a su profunda relación con Facebook.

Gráfico 2: Usuarios Activos (aproximado en millones) por Red social (julio 2018)



Fuente: Statista

Sin embargo, la cuestión de las redes sociales presentadas en el gráfico 2 demanda un análisis económico-político. Si observamos la procedencia nacional de cada una de las empresas mencionadas, se revela una dimensión geopolítica y estratégica fundamental.

En la tabla 1, se utilizaron las veinte empresas con mayor cantidad de usuarios y se las relacionó con su procedencia nacional y su pertenencia propietaria. Las redes sociales con mayor cantidad de usuarios pertenecen a cuatro países, dos de ellos de mayor peso relativo.

Tabla 1: Procedencia y relación propietaria de las redes sociales con mayor cantidad de usuarios activos (2018)

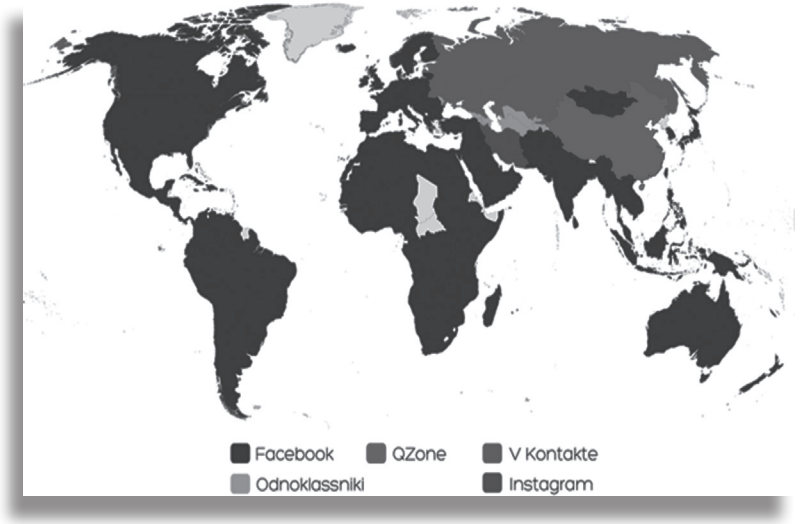
Procedencia	Propietario	Red
China	Tencent	WeChat
		QQ
		Qzone
	Bytedance	Doujin/TikTok
	SinaCorp	Sina Weibo
	Baidu	Baidu Tieba
EE.UU.	Facebook	Facebook
		WhatsApp
		Facebook messenger
		Instagram
	Jack Dorsey	Twitter
	Google	YouTube
	Conde Nast	Reddit
	Microsoft	Skype
		LinkedIn
	Snap Inc.	SnapChat
	Jelly	Pinterest
Japón	Rakuten	Viber
	Line Corp.	LINE
Reino Unido	TM LLP	Telegram

Fuente: Elaboración propia a 2019

Si se hiciera el ejercicio de observar cuál es la red social más usada por país, la dimensión espacial de las redes sociales también cobra un sentido geopolítico.

En el mapa 2 queda plasmada la distribución por país de las principales redes sociales que cada uno utiliza. Resalta rápidamente a la vista: Rusia, China, Irán y algunos países de Asia Central, se encuentran dominados por redes sociales alternativas a las occidentales. Qzone en China, V Kontakte (VK) en Rusia, Odnokiassniki en países de Asia Central. Utilizando la tabla 1, la conclusión demuestra el papel de las empresas de la industria de internet en la geopolítica espacial de las redes sociales.

Mapa 2: Red social más utilizada por país (enero de 2018)



Fuente: Vincos.it

Los ejemplos no han sido desarrollados con exhaustividad y cumplen la función de (re)representar, desde una mirada geopolítica, las dinámicas de las redes sociales y las empresas detrás de ellas. De ninguna forma la discusión debe terminar aquí. En todo caso, se abre el interrogante frente a las dinámicas posibles vinculadas a la gestión de los espacios de interacción y las percepciones cognitivas.

La trascendencia del ciberespacio yace en la capacidad de los usuarios

por medio de acciones directas estructuradas en el lenguaje, la modificación, alteración o disrupción directa de los dispositivos técnicos. Existe una interrelación entre los dispositivos técnicos, su uso social y los medios, en los cuales el mensaje puede modificar cualquiera de los elementos de la ecuación. De esta forma, los nodos –tanto los físicos como los digitales– se constituyen en epicentros estratégicos para el control, regulación o difusión de la circulación de la información sea maliciosa, falsa o verdadera.

Lo nodal de distintos espacios hace al potencial de "viralización" de distintos tipos de contenidos al ser los puntos de confluencia de distintos usuarios. Básicamente, la viralización de un contenido consiste en la rápida difusión interindividual gracias a las posibilidades de interconexión y velocidad de retransmisión de un mensaje que facilita internet.

En este sentido, el ciberespacio se encuentra compuesto por múltiples espacios y medios de relacionamiento, de interpretación cognitiva mediados por el lenguaje. La espacialidad yace en la existencia o no de individuos en determinadas redes o medios, que pueden acceder a determinado tipo de información o de intercambio colectivo. Al mismo tiempo, el intercambio puede resultar en una modificación propia de las percepciones de los individuos o incluso en la modificación del medio dado un su uso social.

A partir de las posibilidades tecnológicas que permiten dichos mecanismos lógicos-digitales, se estructura una dimensión que articula la relación tanto entre seres humanos como de seres humanos con la infraestructura física. Incluso, se han originado nucleos de interacción, comercio, ocio, aprendizaje, entre otras cosas, puramente digitales. Así, podemos también considerar al ciberespacio como un ámbito digital de interacción humana:

Un ámbito digital de interacción humana, a través del cual se procesan distinto tipo de relaciones entre personas, grupos o Estados. Esta definición aquí propuesta, además de contemplar la naturaleza tecnológica del ciberespacio, nos permite avanzar en los aspectos político-estratégicos derivados de su uso, siendo la formulación de políticas específicas de seguridad y/o defensa, una de sus muchas manifestaciones (Gastaldi *et al.*, 2018, p.8).

De este análisis, se desprende entonces otro elemento que caracteriza al ciberespacio: la transversalidad. La transversalidad del ciberespacio puede abordarse de una forma dual o incluso tripartita, considerando las estructuras físicas que dan lugar a su existencia y las características propias de su existencia como resultado de la interacción entre seres humanos (Castells, 2009). Ciertas dinámicas que ocurren en el ciberespacio pueden afectar di-

rectamente a las estructuras y a los dispositivos técnicos más allá de la gestión de las percepciones sociales, es decir de sus usuarios. En otras palabras, las barreras entre la capa física y lógica-digital se han ido desdibujando, dando lugar a una serie de posibles acciones que permiten la influencia directa del mundo digital en el mundo físico o real, no solamente en los dispositivos técnicos, sino también en la vida personal de los individuos.

El optimismo del futuro –¿o del pasado?– anclado a las nuevas tecnologías de la comunicación, las posibilidades que ofrecían internet y todas las nuevas oportunidades de la llamada cuarta fase de la industrialización, se encuentran así con su lado oscuro: los recientes escándalos que giraron en torno a WikiLeaks, Facebook y Cambridge Analytica, han puesto de manifiesto una problemática severa en cuanto la disponibilidad, el acceso y la utilización de la denominada "Big Data" en la política y el surgimiento de nuevas amenazas y riesgos para las naciones y los individuos.

El dilema, sin embargo, no es aparentemente tan claro: la libertad y la vigilancia de la distribución de información sensible para los gobiernos puede ser identificada desde, al menos, dos perspectivas. La primera, cómo esa información sensible, al ser vulnerada, estaba atacando no necesariamente una infraestructura particular del sistema de poder de muchas naciones, sino que esa divulgación de información pone en jaque equilibrios intra e interestatales. La segunda, cuáles son los instrumentos y las estrategias necesarias para generar mecanismos de defensa frente a las nuevas vulnerabilidades que surgen a raíz de las transformaciones económicas y sociales estructuradas en base al ciberespacio.

El ejercicio del poder yace principalmente en la capacidad de los actores de enmarcar, priorizar y establecer agenda, influyendo directamente en la construcción de las percepciones de los ciudadanos con el mundo que los rodea. De allí surge la fuerza de internet como elemento de propaganda. Pero este poder no sólo alcanza a los individuos que operan o usan la red, sino también a las comunidades de individuos políticamente organizados en un territorio dado: los Estados. Los Estados han encontrado en las operaciones cibernéticas un medio o herramienta para influir en otros Estados, de manera disruptiva, o mediante la degradación o el espionaje (Valeriano, *et al.* 2018). Así, a través del ciberespacio un Estado puede alcanzar sus objetivos políticos sin la necesidad de entrar en combate. En tal sentido, el componente ciber tiene un pepel estratégico en las relaciones internacionales. Tal afirmación la sostienen Borges Gama Neto, Guedes de Oliveira y

Vilar Lopes (2016), quienes plantean la necesidad de que entrado ya el siglo XXI, las Relaciones Internacionales (RRII) deberían considerar un subcampo en la disciplina, denominado CiberRRII, o relaciones internacionales cibernéticas. Así, podemos considerar también la necesidad de avanzar en otros conceptos –además del ya largamente empleado ciberguerra–, como ciberpaz o ciberdiplomacia.

Sin embargo, no son solo los Estados los actores centrales de este escenario estratégico. También tienen papeles significativos pequeños Estados e incluso actores no estatales, ya sea un solo individuo –como el caso de Edward Snowden–, u organizaciones, como pueden ser grupos hacktivistas –WikiLeaks o Anonymous– o grupos criminales y terroristas. Por ello, Joseph Nye (2010) señala correctamente que el ciberespacio se caracteriza por la dispersión del poder: en el ciberespacio existe una multiplicidad de actores que, empleando diversos recursos digitales, explotan vulnerabilidades para imponer su voluntad o influir en determinados eventos, como ha sido, por dar un ejemplo, la presunta intervención de Rusia a través de WikiLeaks en las últimas elecciones presidenciales de los Estados Unidos.

Incluso, surge la necesidad de reflexionar en torno a la capa física que hace posible las interacciones del ciberespacio. Dicha infraestructura implica necesariamente la participación activa de tecnologías estratégicas tanto virtuales como físicas. En este sentido, la cuestión de la autonomía, dependencia e interdependencia cobra un nuevo sentido frente a elementos que no son neutrales ni libres, sino todo lo contrario: obedecen, en última instancia, a intereses de otros actores.

Nuevas herramientas, viejos hábitos

Sin duda, la aparición de WikiLeaks puso de manifiesto algo que para muchos era teóricamente evidente, pero que hasta ese entonces no podía comprobarse por falta de datos: el ciberespacio y la circulación de información en el internet tiene sus costos tanto para los individuos como para los gobiernos.

Sin embargo, el dilema no es tan claro como aparenta: la libertad y la vigilancia de la distribución de información sensible para los gobiernos puede ser identificada desde dos perspectivas. La primera, cómo la sociedad puede anteponerse no solamente a los gobiernos sino a los Estados que son, para

muchos, entidades represivas. La segunda, cómo esa información sensible, al ser vulnerada, estaba atacando no necesariamente a una infraestructura particular del sistema de poder de muchas naciones, sino que esa divulgación de información puso en jaque equilibrios intra e interestatales. Es decir, el interrogante que devela es claro y ha sido fuente de polémica desde hace décadas pero hoy, gracias a las nuevas tecnologías de la información, vale la pena preguntarse hasta qué punto la información secreta y sensible de un Estado debe ser de libre acceso.

El problema no termina aquí. El sistema digital posee la capacidad no solamente de ofrecer un espacio en el cual lo individuos (inter)actúan generando no trabajo, educación o intercambio comercial, entre otras cosas, sino que también permite que todo movimiento u accionar pueda ser almacenado vinculando con la fuente. A gran escala, dicha información puede formar parte de grandes bases de datos que, elaboradas y estudiadas, ofrecen una información invaluable, con capacidades predictivas, de lo que implican los intereses individuales de forma agregada.

La estadística del Big Data en algunas esferas, en particular la de los gustos, los intercambios y los comportamientos de los individuos en el ciberespacio, implican el cruce de fronteras legales y filosóficas que necesitan ser discutidas. Las redes sociales no solo venden pauta publicitaria a quien esté dispuesto a pagar, sino que ofrecen a cambio una capacidad de segmentación de la población en base a comportamientos que son, en gran parte de los sistemas republicanos, pertenecientes a la esfera privada. Es decir, el Big Data de los comportamientos de los individuos en el ciberespacio es parte de un proceso no solamente de operacionalización metodológica y estadística, sino también de un proceso de mercantilización de dicha información.

Dicha circunstancia se volvió evidente con el escándalo de Cambridge Analytica, que terminó por poner a Mark Zuckerberg, creador de Facebook, frente a los legisladores estadounidenses para pedir disculpas por el daño ocasionado. Ahora bien, ¿cuál es dicho daño y su impacto en la realidad?

En las tres horas y media de interrogatorio que le realizaron los miembros del parlamento inglés al CEO de Cambridge Analytica, Alexander Nix, se observa una gran cantidad de preguntas y respuestas que sobrevolaron lo discursivamente vago y ambiguo. Ahora bien, del trabajo de investigación realizado por “Channel 4 News”, videos publicados en internet, se pone de manifiesto el poder implícito y las herramientas ofrecidas por dicha empresa para asegurar la victoria de los candidatos que estuvieran dispuestos a tra-

bajar con ellos: extorsión, noticias falsas, atrapamiento (*entrapment)*, entre otros.

Dichas maniobras no son novedad en la política. Aun así, las campañas sucias hoy cuentan con una herramienta efectiva anclada en una mayor certeza frente a los intereses y las preocupaciones individuales. Si esto es posible, cuando analizamos una empresa como Cambridge Analytica, sería aplicable por una nación frente a otra con intereses particulares. Cambridge Analytica no solamente implica un escándalo corporativo relacionado a herramientas electorales poco éticas, es la punta de un iceberg de un fenómeno de mayor trascendencia política.

De hecho, se han comenzado a replantear fenómenos sociopolíticos de gran relevancia ocurridos en la última década: la Primavera Árabe, el giro a la derecha de Latinoamérica, la invasión de Rusia a Ucrania, entre otros.

Un reciente informe, proveniente de European Political Strategy Centre (EPSC) de la Comisión Europea, pone el énfasis en los desafíos contemporáneos que representan las amenazas contemporáneas en la era digital en cuánto a la intromisión electoral. Dejando de lado los llamados ciberataques, que responden a acciones directas que afectan la integridad de las infraestructuras (críticas o no) o las de los individuos, en "Election Interference In The Digital Age" (EPSC, 2018) se observan varias formas indirectas que contribuyen a la manipulación y que pueden tener un resultado representativo en elecciones con diferencias marginales entre los candidatos.

Como se mencionó anteriormente, en muchos casos involucra la cooptación de elites y/o candidatos que implica en ocasiones incluso la financiación (in)directa. Estos mecanismos se complementan con acciones de manipulación electoral por medio de propaganda en medios digitales, campañas de desinformación, amplificación del afectiva-sentimental (explotando el descontento o la afinidad), la falsificación de identidad, etc.

El mundo digital se convertido en una esfera funcional del accionar psicosocial para el comportamiento de actores con intereses. En definitiva, en el ciberespacio se observa el resurgimiento del tradicional y filosófico dilema libertad-seguridad[2]. Las principales potencias –Rusia, China y Estados Unidos– han articulado una amplia gama de políticas para asegurar y construir hegemonía digital.

Los países desarrollados, tales como India, Alemania, Francia, Inglaterra,

2 Manuscrito en revisión de pares.

etc. Han comenzado a erigir las estructuras necesarias para evitar el socavamiento de las instituciones democráticas frente a estos nuevos riesgos. Incluso el voto electrónico presenta amplias variedades de vulnerabilidades, a tal punto que muchos países han retornado a métodos tradicionales.

Sin embargo, en los países periféricos donde se ejerce el poder hegemónico desde la dimensión digital, la historia se presenta de forma diferente. Allí dónde las estructuras necesarias para poder asegurar la mayor pureza posible de los procesos se encuentran ausentes, los dilemas son otros. Especialmente porque no siempre se observan los medios o la voluntad por el desarrollo. *Ceteris paribus,* al actor que logra su victoria con el favor de una potencia, le conviene mantener oculta su relación con ella.

Orígenes de la instrumentalización política de las redes sociales[3]

"Yo no construí la bomba, solo he demostrado que existe" así afirmó Michal Kosinski (Grassegger y Krogerus, 2017) refiriéndose a la creación del algoritmo que dio lugar a las bases técnicas para la aplicación del Big Data, obtenido de redes sociales, al estudio psicosocial y comportamental de los individuos en ellas. Cabe preguntarse: ¿dónde se halla el mecanismo de transformación de la dinámica social en una herramienta política?

La gran transformación sucedió gracias a la expansión geométrica de obtención y almacenamiento de datos gracias a internet. Big Data significa, en esencia, que todo lo que hacemos, tanto dentro como fuera de línea**,** *deja huellas digitales*. Cada compra que hacemos con nuestras tarjetas, cada búsqueda que hacemos en Google, cada movimiento que hacemos cuando nuestro teléfono celular está en nuestro bolsillo, cada "me gusta" está almacenado. Especialmente cada "me gusta". Durante mucho tiempo, y como principal narrativa, la interacción con el mundo digital facilita el "micro-targeting" haciendo posible la publicidad hiperespecífica. Es decir, podríamos encontrar anuncios de zapatillas justo después de haber buscado en algún buscador "cómo correr más rápido".

3 El siguiente apartado posee como principal fuente el trabajo realizado por Hannes Grassegger y Mikael Krogerus en The Data That Turned the World Upside Down para la Universidad de Stanford (2017).

Sin embargo, eventos de gran envergadura como el accionar de Rusia con sus países en su órbita geopolítica, el ascenso del presidente Trump al poder o la campaña de Brexit pusieron de manifiesto otra lógica de utilización del

Big Data en redes sociales. En Occidente, tanto en las elecciones estadounidenses como en el referéndum en Inglaterra, hubo un factor común: una empresa llamada Cambridge Analytica.

Toda esta cuestión se remonta a unos años atrás: a 2014, en el Centro de Psicometría de la Universidad de Cambridge. La psicometría se enfoca en medir rasgos psicológicos y comportamentales que colaboran para la categorización de la personalidad de los individuos. Hasta entonces, existían modelos y tipologías que carecían de sustento debido a una gran debilidad metodológica: se requiere una gran cantidad de información.

Muchos de estos modelos fueron concebidos hace décadas. Particularmente, el modelo estándar que hoy se utiliza busca evaluar a los seres humanos basándose en cinco rasgos de personalidad, conocidos como los "Cinco Grandes". Estos son: apertura (qué tan abierto a nuevas experiencias), conciencia (cuán perfeccionista), extroversión (qué tan sociable es), amabilidad (cuán considerado y cooperativo) y neuroticismo (si se enoja fácilmente). En inglés, estas dimensiones se conocen como OCEAN (*Openness, Conscientiousness, Extroversion, Agreeableness, Neuroticism*) (Ackerman, 2019)

El puntapié inicial fue cuando Michal Kosinski, aceptado por la Universidad de Cambridge para realizar su doctorado en el Centro de Psicometría, se unió a su compañero de estudios David Stillwell, quien había lanzado una pequeña aplicación de Facebook donde se aplicaba el modelo OCEAN. Dicha aplicación llamada "MyPersonality" les permitió a los usuarios llenar diferentes cuestionarios psicométricos, incluyendo preguntas psicológicas del cuestionario de personalidad de los Cinco Grandes. Sobre la base de la evaluación, los usuarios recibieron un "perfil de personalidad" (valores de los Cinco Grandes individuales) y pudieron optar por compartir sus datos de perfil de Facebook con los investigadores. (Grassegger y Krogerus, 2017).

La sorprendente predisposición de los usuarios a compartir su información personal por medio de dicha aplicación, convirtió a los dos doctorandos en los mayores poseedores del conjunto de datos que combinaba puntuaciones psicométricas con los perfiles de Facebook que se habían recopilado en toda la historia. Dicha situación les permitía obtener deducciones notablemente confiables. Algunos ejemplos que se mencionan en el trabajo realizado por Grassegger y Krogerus (2017): los hombres a quienes les "gustó"

la marca de cosméticos MAC tenían una probabilidad ligeramente mayor de ser homosexuales; uno de los mejores indicadores de la heterosexualidad fue que les "gustara" Wu-Tang Clan. Los seguidores de Lady Gaga eran probablemente extrovertidos, mientras que aquellos que a los que le "gustaba" la filosofía tendían a ser introvertidos.

El modelo de Kosinski fue refinándose incrementalmente, gracias a la amplia capacidad de generar correlaciones a partir de datos extraídos no solo por lo que el usuario manifestaba abiertamente, sino también por sus acciones e interacciones en las redes. Especialmente, a partir de los "me gusta", se podía deducir una gran variedad de hábitos, tendencias, rasgos personales y gustos. Pero dicha circunstancia siguió ampliándose hacia quienes el usuario se dirigía. Se podían deducir rasgos de otros usuarios a partir del comportamiento de un tercero.

Se comenzaron a utilizar otros indicadores, incluso aquellos extraídos de cuando no estamos en línea. Por ejemplo, el sensor de movimiento de los smartphones revela qué tan rápido nos movemos y qué tan lejos viajamos. Los dispositivos que cargamos diariamente son un vasto cuestionario psicológico que constantemente estamos completando, tanto consciente como inconscientemente.

Sin embargo, sobre todo –y esto es clave– también funciona a la inversa: no solo se podía entender a los usuarios, sino que también se pueden usar determinados atributos para buscar perfiles específicos. Lo que Kosinski había inventado era una especie de motor de perfiles. Esto facilitó notablemente la segmentación de audiencias hasta un punto de profundidad y privacidad, que mal utilizada, podría ser peligrosa.

Reflexiones finales

La magnitud en la que se pueden explotar las debilidades de un segmento sensible a determinados estímulos –anteriormente privados– se ha constituido en una posibilidad gracias al acceso y estudio de Big Data Psicosocial. En el ciberespacio, existen perfiles reales y perfiles falsos, datos reales y datos falsos. El espacio digital es un espacio de interacción caótica, donde la autoridad y la experiencia se encuentran subsumidas en un sistema que los individuos –usuarios– no controlan, y si lo hacen, es en un margen muy reducido.

A dicho proceso contemporáneo, Han (2014) lo denomina segunda Ilustración, tomando como referencia a la primera, que buscó romper la subjetividad del conocimiento por medio de métodos científicos y estadísticos, la segunda ilustración transforma todo en datos e información. Cayendo en la misma dialéctica que la primera, que intenta abolir toda subjetividad, la segunda produce un nuevo mecanismo de violencia basado en una falsa claridad o una "barbarie de los datos". En la superficie, los usuarios navegan e interactúan con dispositivos y plataformas que les dan un beneficio aparente a cambio de información personal. Es información permite la transformación del individuo en una gran masa de datos mercantilizable.

El nuevo poder capitalista yace en la creación de plataformas sobre la que los usuarios actúan. En definitiva, las dinámicas propias de la interacción responden a una estrategia comercial y de sustentabilidad de quién estructura el medio. Desde una perspectiva crítica, y tal como menciona Francesca Bria en un panel de Chantam House realizado el 7 de febrero de 2019, existe una tensión entre la democracia participativa y la actividad cívica y política en plataformas que son fundamentalmente comerciales, que además no juzga la validez de la información sino su circulación y la capacidad de producir beneficio económico.

La falta de legislación apropiada y el crecimiento exponencial de los espacios digitales, promovieron una expansión a gran escala de corporaciones que fueron ocupando "áreas de influencias digitales" y crearon plataformas para los usuarios.

Las estrategias de manipulación e injerencia en las dinámicas electorales de los países, muchos de ellos en la periferia, implican una alianza estratégica entre dichas corporaciones y los actores estatales con intereses estratégicos. En el ciberespacio, las categorías binarias abiertas/encubiertas en lo que respecta el accionar de las potencias se desdibujan en formas híbridas de acción.

La principal causa de asimetría es el desarrollo tecnológico-industrial. En la medida en que los países periféricos no logren autonomía tecnológica, será muy difícil saber o comprobar si son sujetos de manipulación o no. Al mismo tiempo, el principal desafío que se encuentra a la hora de abordar un proceso de planificación, desarrollo e implementación de políticas públicas orientadas a la presente problemática, es que se debe afrontar el dilema libertad-seguridad abordado en Gastaldi y Ocón (2019). En definitiva, cualquier política de ciberdefensa debe contemplar una multiplicidad

de cuestiones, que se manifiestan desde lo infraestructural-técnico y sus implicancias estratégicas hasta la visión filosófico-política que debe definir los límites y los alcances del sistema de Defensa Nacional. Ninguna política está nunca libre de tensiones teóricas y prácticas.

Bibliografía

Ackerman, Courtney (2019). "Big Five Personality Traits: The OCEAN Model Explained" en Positive Psychology Program. URL: https://positivepsychologyprogram.com/big-five-personality-theory/

Borges Gama Neto R., Guedes de Oliveira, M. y Vilar Lopez G. (2016). *Relações Internacionais Cibernéticas (CiberRi) Oportunidades e Desafios para os Estúdios Estratégicos e de Segurança Internacional*. Recife: Editora UFPE.

Castells, Manuel (2009). *Comunicación y Poder.* Traducción de María Hernández. Madrid: Ed. Alianza

European Political Strategy Center (2018). *Election Interference in the Digital Age: Building Resilience to Cyber-Enabled Threats.* European Commission.

Gastaldi, Sol, et. al. (2018). Ciberdefensa y soberanía nacional: indagando teorías y definiendo conceptos. *Primeras Jornadas de Ciencia y Tecnología de la Universidad de la Defensa Nacional,* Buenos Aires, 28 de julio.

Grassegger, Hannes y Mikael Krogerus (2017). "The Data That Turned the World Upside Down" en *Stanford Public Policy Program.*

Han, Byung-Chul. *Psicopolítica: Neoliberalismo y nuevas técnicas de poder.* Herder Editorial: 2014

Leiras, Marcelo, Andres Malamud y Pablo Stefanoni (2016). *¿Por qué retrocede la izquierda?* Buenos Aires: Capital Intelectual

Levin, Dov H. (2016). "When the Great Power Gets A Vote: The Effects of Great Power Electoral Interventions on Election Results" en *International Studies Quarterly, 60 (2):189-202*

Nutter John (2000). *The CIA's Black Ops: Covert Action, Foreign Policy, and Democracy*. New York: Prometheus Books

Nye, Joseph S. (2010). *Cyber power.* Cambridge: Bedfer Center for Science and International Affairs.

Gastaldi, Sol y Alfredo Leandro Ocón (2019). "Ciberespacio y Defensa Nacional: Una Reflexión sobre el Dilema Seguridad-Libertad en el Ejercicio de la Soberanía" en *Revista UNDEF n°2 pp 88-108*

U.S Marines Corps (1940). *Small Wars Journal.* Washington: Department Of The Navy.

Valeriano, Brandon, Jensen, Benjamin y Maness, Ryan (2018). *Cyber strategy. The evolving character of power and coercion*. Oxford: Oxford University Press.