Geopolítica en el ciberespacio universitario: agendas internacionales "ocultas" para la captura de información

JUAN CARLOS BARRÓN PASTOR
Universidad Nacional Autónoma de México

Si la guerra fría de 1964 se está librando
con tecnologías de la información
es porque todas las guerras, en todas las culturas,
siempre se han librado con las últimas tecnologías disponibles.

Marshall McLuhan

INTRODUCCIÓN

Dentro de las agendas internacionales de información, están las relacionadas con su captura y procesamiento con fines geopolíticos. Esta actividad se realiza en el ciberespacio a través de los aparatos y las redes que utilizan los medios de comunicación no presencial, los cuales, como ha sido señalado por distintos autores en el último siglo, no sólo fungen como intermediarios, sino como generadores de información en los procesos de emisión, transmisión y recepción de mensajes, y los procesos de codificación y decodificación de éstos (*cf*. McLuhan, 1964).

Autores como Charles Pierce, Claude Shannon, Gregory Bateson y Norbert Wiener han dejado un amplio legado sobre las dificultades en la conceptualización de la información, así como los problemas técnicos, semánticos y cibernéticos que involucra; sus herederos contemporáneos han cultivado un campo prolífico en donde estos temas han sido ampliamente difundidos y discutidos por expertos en sus respectivos campos de investigación. Sin embargo, la captura, el análisis y la generación de nueva información basada en las interacciones informativas que ocurren dentro de una red comunicativa han sido de un interés milenario para los pensadores y estrategas inmersos en el estudio de la guerra.

Dentro de ese campo, los métodos geopolíticos se han planteado en los desafíos que implica la búsqueda del control territorial y poblacional de espacios específicos, desde la apropiación de ciertos recursos en un territorio, el control de la población que allí vive o transita, hasta la capacidad de influencia en la conducción de los dispositivos ideológicos.

Es fácil suponer que con la humanidad nacieron los conflictos y los retos relacionados con el poder y el control de ciertos recursos en espacios terrestres específicos. Hace más de cinco mil años, ciertas civilizaciones comenzaron a disputarse el control de los espacios marítimos, y desde finales del siglo XVIII se comenzó a explorar el control del aire en zonas de combate, en un principio para informarse de los movimientos detrás de las líneas enemigas y así anticipar la defensa, y ya en el siglo XX para crear nuevos horrores tanto en combate como en contra de la población inerme. Ya en ese siglo, los avances tecnológicos llevaron a que un nuevo territorio se contendiera como parte de los enfrentamientos bélicos por el control de los territorios y las poblaciones: el espacio sideral adyacente a nuestro planeta.

A finales de ese mismo siglo, los avances tecnológicos han gestado un nuevo territorio, el ciberespacio, y la disputa actual por su control es clave. El ciberespacio es el "[…] espacio operacional donde los humanos y sus organizaciones usan las tecnologías para actuar y crear efectos […] cuya columna vertebral es el entramado de redes interdependientes e interconectadas que utilizan tecnologías de comunicación-información." (Kuehl, 2009: 5-6; traducción propia).

Como es de esperarse, en este nuevo espacio el poder también se va redefiniendo y se crean nuevas formas para ejercerlo dentro y fuera del ciberespacio. Por ello, el dominio sobre la construcción de la información en sí y de las tecnologías de la información y la comunicación es uno de los factores clave para poder controlar las actividades que no sólo se presentan en el ciberespacio, sino que ahondan la capacidad y la controversia por el control de los espacios y de las personas.

En este capítulo, se busca explorar cómo se conducen, confluyen y disputan algunas de las agendas internacionales de la información en lo que hemos denominado "ciberespacio universitario". Esta especie de no-lugar es donde ocurren las comunicaciones no presenciales de una comunidad adscrita a una institución de educación superior.

En la invitación a participar con este escrito, se exhortaba a que los colaboradores reflexionáramos sobre las agendas internacionales de información. En la línea de investigación que desarrollo actualmente en el Centro de Investigaciones sobre América del Norte (CISAN) de la Universidad Nacional Autónoma de México (UNAM), busco conocer cómo se construyen los imaginarios sociales internacionales en el sistema de medios de comunicación, particularmente los relacionados con la región de América del Norte, en donde se encuentra Estados Unidos, el país militar y mediáticamente

más poderos del mundo. Mi investigación tuvo que transformarse al incluirse en el área de estudios estratégicos. Prácticamente todas las agendas internacionales interactúan en el ciberespacio, y por lo tanto cuentan con la intermediación cada vez más invisibilizada de quienes pelean por el control del ciberespacio. Me parece que mirar más de cerca esta disputa es clave para entender las agendas internacionales de información.

Este capítulo explora brevemente algunos casos recientes de intervención informática en universidades para observar algunas características comunes en la construcción de las agendas internacionales de información. Esta agenda se presenta como "oculta", y se usan las comillas para denotar ironía, pues desde las revelaciones de Snowden y Greenwald parecen operar dentro de una especie de dispositivo en el que la captura de información vía Internet parece tratarse como un mal necesario o, incluso, con desdén. Estos mecanismos de vigilancia y disciplinamiento en el ciberespacio son clave, sin embargo, para entender cuál podría ser el trasfondo de varias de las agendas geopolíticas internacionales que atañen a la discusión que se hace en este volumen.

El ciberespacio universitario como posible blanco geopolítico

De acuerdo con May y Lane (2006), las universidades en general cuentan con tres temas cruciales en características relacionadas, o que deberían estar relacionadas con sus agendas de manejo de la información, pues están relacionadas con su seguridad en el ciberespacio. El primer tema crucial que ellos señalan es que las universidades albergan una

gran variedad de sistemas informáticos (académicos, administrativos, comerciales, de propiedad intelectual, de interés periodístico o político, etcétera) que funcionan como portales, espacios de convergencia de información, centros de generación de información cuyo manejo requiere de gran cuidado y prudencia, o incluso, como rutas de tránsito privilegiado para el intercambio de información sensible. El segundo tema crucial que indican es que las universidades son un espacio fundamental para el "cultivo", el desarrollo y la investigación relacionada con las tecnologías de la información. En tercer lugar, estos autores mencionan que, desde una perspectiva industrial, las universidades son una fuente primordial de futuros líderes e innovadores.

Además de los tres temas señalados, podemos incluir en esta reflexión uno más: Roelofs y Gallien (2017) recuerdan que la tiranía y las posibles contradicciones que nos imponen en la academia las clasificaciones de citas (*citation rankings*) pueden ser consideradas como otra modalidad de *hackeo*, o incluso como una forma de corrupción, diría yo. Esta agenda, promovida por prácticamente todas las instituciones académicas, busca que la producción académica y científica "impacte" en la sociedad y mida qué tan importante o valioso podría ser un artículo académico en función de qué tanto se habla de él en redes sociales, o cuantas veces es citado.

Por un lado, plataformas como Scopus, Web of Science o Google Scholar ofrecen un conteo de citas como parte de su modelo de negocios; por el otro lado, sistemas de valoración académica como el Sistema Nacional de Investigadores del Consejo Nacional de Ciencia y Tecnología de México (SNI-CONACyT), por ejemplo, parecen cada vez más confundir la relevancia o la seriedad de una publicación en función de esos conteos. Para Roelofs y Gallien, estos artículos provo-

cadores cuentan con la capacidad para *hackear* la actividad académica por la vía de crear falsos disensos, dar visibilidad a investigaciones poco rigurosas, o involucrar a los académicos en discusiones tangenciales que pueden mantenerlos entretenidos en aspectos poco relevantes, en lugar de continuar enfocándose en estudiar temas decisivos para nuestras sociedades o el planeta.

En 2009, la University of East Anglia (UEA, universidad en la que cursé mis estudios de maestría y doctorado) fue objeto de un ataque informático. Centenares de mensajes electrónicos y archivos adjuntos enviados por correo fueron intervenidos y capturados por hackers. La información se hizo llegar a la prensa británica primero y después al resto del mundo, como una muestra de que algunos investigadores que estudian cuestiones relacionadas con el cambio climático, supuestamente, habrían conspirado para privilegiar la publicación de una investigación que prueba el impacto del modo de producción en el cambio climático, en detrimento de artículos que sostienen que la actividad humana no es tan relevante para el cambio climático, o que, incluso, el cambio climático en sí podría no estar ocurriendo del modo en el que generalmente se piensa.

Visto este acontecimiento casi una década después, este ataque informático y su respectiva filtración en la prensa trajo consigo al menos tres cuestiones que afectan a las agendas internacionales de la información y que tienen implicaciones geopolíticas:

1. La construcción mediática de que los científicos no se han puesto de acuerdo en torno a los fenómenos relacionados con el cambio climático que estamos viviendo, y de ahí, con un salto mental temerario que difícilmente podríamos considerar lógico, pare-

ce concluirse que el cambio climático podría ser una gran mentira con la que buscan manipularnos ciertas élites políticas adversarias a nuestros intereses.
2. Que los hackers obedecen a los intereses del gobierno ruso y que buscan desestabilizar las instituciones políticas de sus adversarios y de prácticamente todos los países del orbe, a la vez que van "confirmando" diversas teorías de la conspiración.
3. Que estos ataques informáticos parecen traer consigo el mensaje de que es necesario mantener y fortalecer aparatos de vigilancia y control estadounidense supranacional sobre Internet, como la Agencia de Seguridad Nacional de Estados Unidos (NSA).

Un vistazo a la Sociocibernética crítica

En años recientes, como parte de mi proyecto de investigación en el Centro de Investigaciones sobre América del Norte de la Universidad Nacional Autónoma de México (CISAN-UNAM), he venido desarrollando una propuesta teórica y metodológica para estudiar los sistemas, en particular el sistema de medios de comunicación no presencial, que he llamado "Sociocibernética crítica". Esta propuesta la he comenzado a desplegar en otros escritos ya publicados o en proceso de publicación (Barrón, 2018). Ofrezco una disculpa al lector por la autoreferencia y por lo apresurado de esta sección, pero a la vez de que me parece necesaria su mención, me parece menester no repetir lo que en otro lado ya se ha dicho.

La Sociocibernética crítica es una propuesta en ciernes que busca hacer una síntesis de la Sociocibernética, que es una corriente al interior de la Teoría de los sistemas aplica-

da a la conducción de los sistemas sociales. Por otro lado, es una lectura personal de algunas de las discusiones que se han dado dentro de la llamada Teoría Crítica. Esta construcción teórica ha buscado contar con un andamiaje metodológico geopolítico; es decir, tomar en cuenta dimensiones espaciales en distintas escalas relacionadas con las problemáticas que surgen de buscar controlar o conducir a una población específica en un territorio.

Con esta propuesta, se busca entender problemáticas propias de la conducción de los sistemas sociales tomando en cuenta ciertas dinámicas de apropiación, despojo, extracción, opresión y sometimiento ejercidas por ciertos actores y elementos que funcionan tanto dentro de ese sistema como en su entorno. A la vez, se busca observar y reflexionar lo que permanece y se transforma en espacios específicos y en distintas escalas, en este caso, el ciberespacio, debido a los esfuerzos conductores, controladores, apropiadores y/o a las disputas, desmantelamientos, resistencias y rebeliones que suceden al interior de los sistemas en interacción con esos espacios.

El ciberespacio es un espacio propio de la interacción no presencial que ocurre dentro del sistema de medios de comunicación y es un elemento clave para la reproducción del poder tanto dentro de este sistema como en su entorno. Buena parte de las agendas internacionales de la información suceden de manera no presencial, y por lo tanto requieren de un intermediario que no sólo realiza labores de intermediación, sino que también es un jugador clave que pretende invisibilizarse para ejercer su poder con mayor margen de maniobra. Los programas informáticos, que son clave para esas agendas, pueden inscribirse dentro de los campos programáticos propios del funcionamiento de este sistema, cuyas interacciones sistémicas nos proponemos es-

tudiar en lo que hemos llamado los campos programáticos de lo que acontece y lo que se conecta. En la siguiente sección, se buscará hacer un ejercicio práctico dentro de este marco teórico.

Las agendas internacionales en la disputa por el ciberespacio universitario

Decíamos que en el ciberespacio universitario cohabitan y se disputan numerosas agendas informáticas. Esto ocurre en parte porque en este ciberespacio coexisten sistemas informáticos relacionados no sólo con las actividades académicas sustanciales al quehacer universitario, sino también con otras labores necesarias para el funcionamiento de las universidades, como las administrativas, las comerciales y las políticas. Paralelamente, en el ciberespacio universitario conviven quienes están desarrollando estos sistemas informáticos y se están formando quienes potencialmente lo innovarán y transformarán. Además, parece haber varias agendas que buscan que la contabilización de citas se convierta en un indicador de validez y en donde la divulgación adaptada a códigos periodísticos sensacionalistas se puede percibir más como una necesidad que como un riesgo para la evaluación de las investigaciones y de los investigadores. Por último, se ha mencionado que parece haber una agenda que promueve que el ciberespacio universitario cuente con sistemas de vigilancia por nuestra propia seguridad y que seamos los propios académicos quienes lo validemos, en protección de posibles intereses rivales internacionales reales o imaginarios.

Estas agendas surgen cada vez más inherentes al funcionamiento del sistema educativo, y en particular al de las

universidades. Podemos ver en el ciberespacio universitario una confluencia de agendas informáticas en donde se libran disputas y hay cooperaciones entre ellas. Esto seguramente está abonando al fortalecimiento de ciertas dinámicas y actores al interior de los espacios y los sistemas educativos, y al debilitamiento de otros actores que tradicionalmente suelen dominar otras áreas o actividades del quehacer académico en general y de las universidades en particular.

Para identificar quiénes son unos y otros, pudiera ser recomendable ir más allá de las tentaciones dualistas y visualizarlas desde una perspectiva de complejidad. Agendas como las mencionadas van empujadas por distintos actores montados en dinámicas "naturalizadas" o dadas como evidentes en aras de mantenerse, por ejemplo, a la vanguardia tecnológica, o transparentar ciertos procesos, informaciones o decisiones a ciertos actores, y ocultárselos selectivamente a otros.

Las interacciones en el ciberespacio universitario, tanto de los actores como de las agendas que hemos identificado, van ocurriendo en los dominios de quienes controlan no sólo el ciberespacio en sí, sino también de quienes controlan los artefactos físicos y energéticos sin los cuales el ciberespacio no sería posible. Es decir, los servidores, los cables y las computadoras, pero también la generación y transmisión de la energía eléctrica sin la cual nada de lo anterior puede funcionar.

Quienes controlan los flujos de los procesos administrativos e informáticos que suceden en el ciberespacio universitario van abriendo o cerrando accesos, permitiendo que ciertas personas puedan tener acceso temporal controlado a ciertas partes específicas de los procesos durante un tiempo delimitado por "el sistema". Su funcionamiento se asemeja a una red de válvulas que se cierran y se abren selectivamente. Parece importante volver a subrayar que estos meca-

nismos de conducción sistémica para las distintas agendas informáticas no sólo pasan en las actividades académicas sustanciales al quehacer universitario, sino posiblemente de manera primordial en las "otras" labores necesarias para el funcionamiento de las universidades como las administrativas, las comerciales y las políticas.

Desde luego, la información que se encuentra en el ciberespacio universitario tanto en términos de investigación o de propiedad intelectual, como las que pueden potencialmente ser de interés periodístico o político, así como el robo de recursos financieros, o la piratería de datos, metodologías e incluso procedimientos administrativos o legales, puede ser valorada en términos económicos, políticos, o militares y, por lo tanto, ser susceptible de que alguien ponga un precio sobre su captura.

El espionaje ha sido desde hace siglos una de las tareas bélicas medulares para la captura, el análisis y la generación de nueva información confiable que sirva para anticipar las acciones de quienes contienden por el control de un espacio. En su modalidad de ciberespionaje, ha involucrado tareas como la infiltración en centros de generación de conocimiento públicos y privados, robo de información relacionada con propiedades industriales, diseños o marcas; pirateo de bases de datos y materiales en proceso de investigación; acceso ilegal a información privada, conversaciones, imágenes o correos de las personas para luego exhibirlas y/o chantajearlas, y sustracción datos personales y bienes monetarios vía electrónica. Esto está generando en la actualidad intrincadas redes informáticas ofensivas y defensivas, así como mecanismos cada vez más complicados para encriptar y desencriptar la información que se encuentra en el ciberespacio en general, y en el ciberespacio universitario en particular.

Antes de cerrar, y aunque es un tema al margen de lo que se ha tratado en este capítulo, podría ser interesante recalcar el lugar común en que se ha reeditado la representación mediática en relación con los hackers rusos. Sin menoscabo de lo que pueda haber de cierto detrás de la información de que el gobierno de Rusia haya estado o no detrás de las intervenciones en los procesos políticos de otros países, particularmente en la elección estadounidense de 2016, también es verdad que Estados Unidos, y muy posiblemente otros países, ha intervenido abiertamente en procesos electorales y ha organizado golpes de Estado. Estados Unidos ha sido un actor clave en el encumbramiento de actores políticos afines a la postura de Washington en todo el planeta por la vía de la intervención encubierta y muchas veces de manera no muy discreta.

Aun así, con actualizaciones de algunos elementos macartistas de la Guerra Gría, la cobertura mediática relacionada con ciberataques pareciera querer machacar con la idea de que los hackers rusos están detrás de muchos de los ciberataques actuales. Así, se ha señalado a los Servicios de Seguridad de Rusia en conjunto con la llamada Red de Negocios Rusos como los principales responsables de los ciberataques en contra de Estonia en 2007, o los que se llevaron a cabo para hacer frente a Georgia luego de la independencia de Osetia del Sur en 2008, o atacando universidades como la ya mencionada UEA en 2009, aparentemente para guardar la información robada en servidores ubicados en Siberia (*cf*. Karatgozianni, 2010). Más recientemente, y continuando con la reiteración de ciertos elementos de la Guerra Fría, Rusia ha sido señalada en diversas ocasiones de realizar ciberataques en contra de las instituciones políticas adscritas a la Organización del Tratado del Atlántico Norte para promover el Brexit y la independencia de Cataluña,

para intervenir en el proceso electoral estadounidense, e incluso ya se usan representaciones mediáticas de los hackers rusos para difundir en México la idea de que Rusia influyó en el proceso electoral mexicano de 2018.

No es éste el lugar ni la investigación para determinar qué tan ciertas o exageradas sean esas narrativas mediáticas que han proliferado en torno a las intervenciones rusas en el ciberespacio. Pero, sin duda, simbolizar mediáticamente a Rusia como una nación de super-hackers y la representación mediática que podríamos denominar "hackers rusos", ya parece haberse adoptado como un lugar común al que se podrá recurrir prácticamente en cualquier caso en el que la seguridad en el ciberespacio se vea comprometida. Deberemos estar alertas y ser escépticos, pues culpar a los rusos ya es una estrategia probadamente efectiva para encubrir algunas facetas potencialmente criminales de las agendas internacionales para el robo de información y el espionaje en el ciberespacio.

A MANERA DE CONCLUSIÓN

En este capítulo se han revisado desde una perspectiva geopolítica algunas agendas internacionales de la información que confluyen actualmente en el ciberespacio universitario. Para ello, se identificaron algunas dinámicas que podemos observar en el quehacer cotidiano de quienes nos dedicamos a la investigación académica.

Las dinámicas que se señalaron a lo largo de este capítulo tuvieron que ver con la gran variedad de sistemas informáticos que confluyen en el ciberespacio universitario y de cuya coexistencia y conflicto podemos inferir ciertas agendas internacionales, tales como los muy controvertidos

mecanismos de evaluación a los que estamos siendo sometidos los investigadores y los profesores en México y en buena parte del mundo. Asimismo, se revisó cómo algunas de estas agendas internacionales pueden estar ayudando a instrumentar falsos consensos y disensos en torno no sólo a ciertos temas de actualidad como el cambio climático, sino sobre todo a la naturalización de los procesos informáticos para que la vida académica sea impensable sin ellos.

Las agendas internacionales de la información pueden estudiarse como parte de las interacciones y los mecanismos que ocurren al interior de los campos programáticos del sistema de medios de comunicación no presencial en el ciberespacio. Esta visión sistémica de la posible reproducción auto-organizada de estas agendas informáticas no se puede pasar por alto. Ahondar en estas exploraciones utilizando herramientas como la Sociocibernética crítica podría ayudar a estudiar e ir haciendo aportaciones desde una perspectiva de complejidad para complementar el entendimiento de ciertos fenómenos, como los que se han tratado en este capítulo.

Finalmente, parece importante señalar que entre las repercusiones en los estudios de la información es importante considerar cuestiones de geopolítica internacional. El ciberespacio universitario está generando información de muy diversa índole, no sólo la que estamos buscando generar a propósito, sino en mucha mayor medida, información que sirve a agendas no académicas, y resulta importante reflexionar sobre ello. Es decir, la información que generamos consciente o inconscientemente puede estar siendo utilizada con fines comerciales, políticos o militares. Es por lo anterior que, entre las agendas internacionales de la información, no sólo se cuentan aquellas que buscan gene-

rarla o conducirla, sino también las que buscan vigilarla y controlarla e incluso sabotearla o robarla.

Referencias bibliográficas

Barrón Pastor, J. C. (2018). *Sociocibernética crítica: Un método geopolítico para el estudio estratégico del sistema de medios de comunicación no presencial en América del Norte*. México: UNAM / CISAN.

Karatgozianni, A. (2010). Blame It on the Russians: Tracking the Portrayal of RussianHackers during Cyber Conflict Incidents. *Digital Icons: Studies in Russian, Eurasian and Central European New Media*, (4): 127-150. [en línea], https://www.researchgate.net/profile/Athina_Karatzogianni/publication/259850767_Blame_it_on_the_Russians_Tracking_the_Portrayal_of_Russians_During_Cyber_Conflict_Incidents/links/53fdfc380cf2364ccc09d2bf.pdf

Kuehl, D. (2009). From Cyberspace to Cyberpower: Defining the Problem. En F. D. Kramer, S. Starr y L. K. Wentz (Eds.). *Cyberpower and National Security* (pp. 24-42). Washington: National Defense University Press.

McLuhan, M. (2009). *Comprender los medios de comunicación: Las extensiones del ser humano*. Barcelona: Paidós.

May, L. y Lane, T. (2006). A Model for Improving e-Security in Australian Universities. *Journal of Theoretical and Applied Electronic Commerce Research*, *1*(2): 90-96 [en línea], http://www.redalyc.org/html/965/96510209/

Roelofs, P. y Gallien, M. (2017). Clickbait and impact: how academia has been hacked. Impact of Social Sciences Blog [en línea], http://blogs.lse.ac.uk/impactofsocialsciences/2017/09/19/clickbait-and-impact-how-academia-has-been-hacked/