ieee.es
Instituto Español de Estudios Estratégicos

Documento
Opinión

66/2017 19 de junio de 2017

*Manuel R. Torres Soriano**

Hackeando la democracia:
operaciones de influencia
en el ciberespacio

Hackeando la democracia: operaciones de influencia en el ciberespacio

Resumen

El propósito de este artículo es analizar cómo el nuevo contexto político y tecnológico ha impactado en el desarrollo de las acciones estatales orientadas a influir en el desarrollo de procesos electorales de otros países. A partir del estudio de las elecciones presidenciales de Estados Unidos en 2016, y Francia en 2017, se analizan las causas que explican el éxito o fracaso de los «operaciones de influencia», y se aportan algunas de las lecciones aprendidas de estos dos casos.

Abstract

The purpose of this article is to analyze how the new political and technological context has impacted on the development of state actions aimed at influencing the development of electoral processes in other countries. Using the study of the United States presidential elections in 2016 and France in 2017, this work analyses the causes that explain the success or failure of "influence operations", and propose some of the lessons learned from these two cases.

Palabras clave

Elecciones, servicios de inteligencia, opinión pública, ciberespacio, Rusia.

Keywords

Elections, intelligence services, public opinion, cyberspace, Russia.

Introducción

La teoría política suele describir a la democracia como un sistema de gobierno frágil, que debe ser permanentemente protegido de múltiples peligros. Uno de ellos son las interferencias ejercidas por actores ajenos a la comunidad que ostenta la soberanía, con el propósito de inclinar los resultados del proceso político hacia un resultado que favorezca sus intereses. La necesidad de salvaguardar la independencia del cuerpo electoral ha llevado a múltiples Estados a incluir cláusulas en su diseño constitucional que inciden sobre la financiación, la subordinación externa de los partidos políticos, la acción de los medios de comunicación, etc. Este tipo de medidas encontraron su legitimación dentro del contexto histórico de la Guerra Fría, donde tanto Estados Unidos como la Unión Soviética percibieron que la celebración de elecciones en terceros países podía ser una oportunidad para ampliar su área de influencia y debilitar la del adversario.

Este tipo de injerencias solo podrían resultar exitosas si pasaban desapercibidas a la opinión pública, de ahí que su ejecución fuese encomendada preferentemente a los servicios de inteligencia, los cuales poseían el *expertise* y los medios necesarios para operar de manera encubierta y ofrecer una negación plausible. Las llamadas «operaciones de influencia» recibirían un amplio desarrollo doctrinal y operativo por parte de la Rusia comunista. El fin de la Guerra Fría no supuso la desaparición de estas prácticas, sino que se adaptaron al nuevo contexto geopolítico y a las nuevas oportunidades ofrecidas por la innovación tecnológica. La eclosión del llamado ciberespacio, como un nuevo dominio donde se proyecta el poder estatal, ha proporcionado a las operaciones de influencia una nueva «edad de oro».

El propósito de este artículo es reflexionar sobre cómo el nuevo contexto político y tecnológico ha impactado en el desarrollo de las acciones estatales orientadas a influir en el desarrollo de procesos electorales de otros países. A partir del análisis de las elecciones presidenciales de Estados Unidos en 2016, y Francia en 2017, se analizan los condicionantes que explican el éxito o fracaso de los «operaciones de influencia».

La escuela soviética

El deseo de exportar la revolución socialista y debilitar a sus enemigos exteriores explica por qué, desde un primer momento, el nuevo Estado soviético[1] encomendó a sus servicios secretos la puesta en marcha de una extensa campaña de acciones encubiertas. Este tipo de prácticas fueron bautizadas por la URSS como «desinformación», *kompromat*, «subversión», mientras que en Estados Unidos fueron conocidas como «medidas activas», las cuales llegarían a convertirse en uno de los principales cometidos de estas organizaciones, rivalizando en importancia con las labores tradicionales de obtención de información sobre el enemigo.

Los servicios de inteligencia del bloque comunista, especialmente la KGB, hicieron un amplio uso del engaño para difundir informaciones robadas, parcialmente ciertas, o completamente «fabricadas». Se estima que durante toda la Guerra Fría, la URSS y sus satélites llevaron a cabo más de 10.000 operaciones de desinformación[2] destinadas a socavar la legitimidad de los Gobiernos enemigos, fomentar la contestación interna o provocar desorientación entre la opinión pública. Una de sus creaciones más exitosas fue, por ejemplo, aprovechar la alarma social provocada por la propagación sin control de la enfermedad del SIDA para propagar el rumor de que este virus había sido creado en los laboratorios militares estadounidenses[3].

Con la caída del muro de Berlín, y la consiguiente debilidad política de Rusia, se produjo un declive de este tipo de intervenciones en el exterior. Las operaciones de influencia fueron reorientadas[4] hacia los opositores internos y al apoyo de la intervención militar en la república rebelde de Chechenia, en particular contra la incipiente presencia en internet de los insurgentes islamistas. Sin embargo, a finales de la primera década del nuevo milenio, las operaciones de influencia recobraron el brío

[1] ALEXANDER, Keith B. «Disinformation: A Primer in Russian Active Measures and Influence Campaigns». Prepared Statement before the United States Senate Select Committee on Intelligence, March 30, 2017, disponible en https://www.intelligence.senate.gov/sites/default/files/documents/os-kalexander-033017.pdf. Fecha de la consulta 02/06/2017.

[2] RID, Thomas. «Disinformation: A Primer in Russian Active Measures and Influence Campaigns». Prepared Statement before the United States Senate Select Committee on Intelligence, March 30, 2017, disponible en https://www.intelligence.senate.gov/sites/default/files/documents/os-trid-033017.pdf. Fecha de la consulta 02/06/2017.

[3] BOGHARDT, Thomas. «Soviet Bloc Intelligence and Its AIDS Disinformation Campaign». *Studies in Intelligence,* vol. 53, n.º 4 (December 2009), pp. 1-24, disponible en https://www.cia.gov/library/center-for-the-study-of-intelligence/csi-publications/csi-studies/studies/vol53no4/pdf/U-%20Boghardt-AIDS-Made%20in%20the%20USA-17Dec.pdf. Fecha de la consulta 02/06/2017.

[4] WILLIAMS, Brad D. «How Russia adapted KGB 'active measures' to cyber operations, Part II». *Fith Domain Cyber*, March 20, 2017, disponible en http://fifthdomain.com/2017/03/20/how-russia-adapted-kgb-active-measures-to-cyber-operations-part-ii/. Fecha de la consulta 02/06/2017.

de décadas atrás, apuntando de nuevo a los objetivos tradicionales de la desinformación soviética: Estados Unidos y sus aliados[5].

Una de las adaptaciones de esta nueva etapa tuvo que ver con el tipo de actores que ofrecen una negación plausible, o ejercen un papel decisivo en la propagación de la «desinformación». El antagonismo ideológico de la Guerra Fría era un terreno propicio para que la inteligencia soviética pudiese recurrir a las colaboraciones de actores occidentales que simpatizaban con la causa soviética. Así, por ejemplo, el activismo político en contra del despliegue de misiles nucleares estadounidenses en Europa, podía ser ejercido tanto por pacifistas que de manera sincera abogasen por el desarme unilateral, como por oportunistas de la izquierda radical que aprovechaban cualquier posibilidad de socavar las políticas del bloque capitalista. La desintegración de la URSS también desactivó el «poder blando» que podía ejercer el comunismo como modelo alternativo de organización política y social. La Rusia actual tiene una reducida capacidad para movilizar de manera altruista a activos dentro del ámbito occidental, de ahí que haya hecho hincapié en la figura del «tonto útil» (según el argot de la propia inteligencia rusa): actores que no son conscientes de que han sido instrumentalizados para alcanzar un objetivo distinto al que creen perseguir.

En este nuevo contexto, Rusia ha hecho uso de tres agentes involuntarios: Wikileaks, las redes sociales de Internet y un sector de la prensa dispuesto a publicar cualquier información filtrada sin cuestionar su origen e intencionalidad[6]. En el primer caso, la plataforma basada en la filosofía de la transparencia radical, fue adquiriendo progresivamente un sesgo antiestadounidense, especialmente desde que su fundador, Julian Assange, atribuyó sus problemas legales y su exilio forzoso en la Embajada de Ecuador en Reino Unido, a una campaña orquestada por Estados Unidos para neutralizarle. La predisposición de Wikileaks para publicar cualquier dato perjudicial para el Gobierno americano, sin cuestionar excesivamente su procedencia, llevó a algunos analistas a considerar que la plataforma se había convertido *de facto* en la perfecta «máquina de blanquear las filtraciones rusas», atribuyendo un halo de

[5] GALEOTTI, Mark. «Putin's hydra: Inside Russia's intelligence services». *Policy Brief ECFR,* May 11, 2016, disponible en http://www.ecfr.eu/page/-/ECFR_169_-_PUTINS_HYDRA_INSIDE_THE_RUSSIAN_INTELLIGENCE_SERVICES_1513.pdf. Fecha de la consulta 02/06/2017.

[6] TUCKER, Patrick. «How Putin Weaponized Wikileaks to Influence the Election of an American President». *Defense One,* July 24, 2016, disponible en http://www.defenseone.com/technology/2016/07/how-putin-weaponized-wikileaks-influence-election-american-president/130163/. Fecha de la consulta 02/06/2017.

credibilidad y relevancia a informaciones obtenidas de manera ilegítima por actores que persiguen objetivos muy distintos a los de la democratización del conocimiento.

En el segundo caso, las principales redes sociales, especialmente twitter, fueron utilizadas, no solo como mecanismo para la distribución de las informaciones o consignas, sino también como escenarios en las cuales construir artificialmente mayorías sociales que condicionen el posicionamiento de la opinión pública sobre determinadas cuestiones. La inteligencia rusa hizo un amplio uso de *bots*, cuentas semiautomatizadas y *trols* profesionales para ampliar el alcance y relevancia de determinadas posturas, así como para hostigar a los usuarios discrepantes. La colaboración involuntaria de estas empresas radica en su resistencia a facilitar información sobre el volumen real y la identidad de estos mecanismos automatizados que permiten manipular la *twitteresfera*, y por extensión como percibe una sociedad las posiciones mayoritarias. Ninguna empresa que base su negocio en la venta de publicidad, tiene demasiados incentivos para reconocer que buena parte de sus usuarios y la actividad de los mismos tienen un origen artificial.

En último lugar, las operaciones de influencia rusa pudieron rentabilizar una nueva configuración del panorama mediático internacional. La eclosión de Internet como fuente de información, la crisis económica de los medios tradicionales y la multiplicación de nuevas cabeceras informativas de base exclusivamente virtual crearon un terreno mucho más receptivo para las operaciones de influencia. Durante la Guerra Fría, los intentos de instrumentalizar a la prensa dependían de la habilidad de los servicios de inteligencia de seleccionar, elaborar y enmascarar la desinformación para que esta pudiese superar los filtros editoriales de los distintos medios, los cuales generalmente mostraban unas elevadas reticencias a la publicación de informaciones interesadas, especialmente si podían estar vinculadas con el enemigo comunista. En el nuevo panorama mediático, caracterizado por la descapitalización de las plantillas periodísticas y una agresiva competencia por ingresos cada vez más escasos, han proliferado actores dispuestos a publicar de manera agresiva cualquier información que tenga como origen una filtración, sin reparar en cómo ha sido obtenida la misma, o las posibles motivaciones de quién ha sacado a la luz esa información. Su carácter gratuito y su indudable capacidad de capturar la atención pública se han convertido en las puertas de entrada para que la inteligencia rusa goce de un acceso sin precedentes a la opinión pública.

En definitiva, desde la óptica rusa, siguen resonando las palabras de uno de los históricos responsables de las operaciones de desinformación del KGB, el general Ivan Agayants, el cual declaraba en 1965: «Algunas veces me sorprendo de lo fácil que es jugar a este juego. Si ellos no tuviesen libertad de prensa, deberíamos inventársela»[7].

Estados Unidos: la tormenta perfecta

Estados Unidos era a finales de 2016 una sociedad altamente polarizada en torno a diferentes brechas relacionadas con la raza, la respuesta al terrorismo yihadista, los efectos de la crisis económica, o la propia identidad del país frente al mestizaje socio-cultural provocado por la inmigración de origen principalmente latino. La campaña presidencial aumentó la visibilidad de estas fracturas sociales, especialmente en un sector del electorado que sentía que la «corrección política» de la era Obama había sofocado las reivindicaciones legítimas de una parte mayoritaria de la sociedad estadounidense. Este clima se vio enardecido por la elevada animadversión personal que despertaba Hillary Clinton entre los conservadores, lo cual permitió que determinadas noticias falsas difundidas desde portales de noticias «alternativos» tuviesen un enorme recorrido entre aquellos que estaban dispuestos a creer cualquier relato perjudicial para la candidata demócrata.

Se daban así las condiciones idóneas para que, según el viejo manual de los servicios de inteligencia rusos, tuviese éxito una operación de influencia. Por un lado, los portales de *fake news* y sus *bots* en redes sociales se encargaron del apartado de «desinformación» con la publicación de una retahíla de noticias difamatorias sobre Hillary: que la senadora padecía y trataba de ocultar la enfermedad de Parkinson, que había asesinado a un asistente, o que frecuentaba un club para pedófilos oculto en el sótano de una pizzería de la capital estadounidense[8].

De manera sistemática, los diferentes órganos de la inteligencia rusos penetraron las redes informáticas de los dos grandes partidos políticos estadounidenses, sus candidatos y organizaciones vinculadas. Un año antes de la celebración de las elecciones, el FBI ya había alertado al Comité Demócrata de la necesidad de revisar

[7] RID, *op. cit.* 2.
[8] CALABRESI, Massimo. «Inside Russia's Social Media War on America». *Time,* may 18, 2017, disponible en http://time.com/4783932/inside-russia-social-media-war-america/?xid=tcoshare. Fecha de la consulta 02/06/2017.

sus redes ante la posibilidad de que hubiesen sido infiltradas por un actor hostil[9]. El partido recurriría a los servicios de la empresa de ciberseguridad CrowdStrike[10], que pudo comprobar cómo la información digital de la campaña había sido comprometida por al menos dos grupos distintos de *hackers*, los cuales se habían apropiado de miles de archivos y correos electrónicos del personal demócrata. Según la investigación, la huella digital conducía a grupos vinculados con el Estado ruso, los cuales habían hecho uso de procedimientos idénticos en otras operaciones previas de apropiación fraudulenta y filtrado de información. La empresa establecía que los dos grupos estaban vinculados a dos órganos diferentes de la inteligencia rusa: el grupo apodado como Fancy Bear estaría ligado al GRU (inteligencia militar) y el grupo denominado Cozy Bear estaría vinculado al FSB (inteligencia civil). A través de procedimientos bastante rudimentarios de suplantación de identidad («ingeniera social»), los *hackers* consiguieron acceder a las comunicaciones digitales de un número considerable del personal de campaña de la senadora Hillary Clinton, incluyendo su círculo más próximo. Ambos grupos habían actuado sobre el mismo objetivo sin aparente coordinación y en desconocimiento de las actividades del otro, lo que evidenciaba la importancia que Rusia otorgaba a este tipo de operaciones, hasta el punto de duplicar el encargo en servicios de inteligencia diferentes.

El escándalo de la infiltración rusa llegó a los principales medios de comunicación del país. Tan solo un día después de la publicación de esta noticia, un *hacker* que se hacía llamar Guccifer 2.0, publicaba en Internet un alegato en el que se atribuía la autoría de la apropiación y filtración de los documentos del Partido Demócrata, el cual describía como un «proyecto personal» sin vinculación con ningún país. Para acreditar esta teoría publicó una nueva serie de documentos de este partido, aunque señalaba que la mayoría habían sido entregados al portal Wikileaks. Guccifer mostró una gran insistencia a la hora de desacreditar la vinculación rusa de estas filtraciones, e incluso se ofreció a interactuar digitalmente con los periodistas que quisieran obtener más detalles. Estos contactos, lejos de dar el resultado deseados por Guciffer, mostró las

[9] RID, Thomas. «How Russia Pulled Off the Biggest Election Hack in U.S. History». *Esquire,* October 20, 2016, disponible en http://www.esquire.com/news-politics/a49791/russian-dnc-emails-hacked/. Fecha de la consulta 02/06/2017.

[10] ALPEROVITCH, Dmitri. «Bears in the Midst: Intrusion into the Democratic National Committee». *Crowdstrike Blog,* June 15, 2016, disponible en https://www.crowdstrike.com/blog/bears-midst-intrusion-democratic-national-committee/. Fecha de la consulta 02/06/2017.

incoherencias y debilidades de esa reivindicación individual[11], y fue desacreditado por las autoridades estadounidenses como una campaña orquestada por los propios servicios rusos para generar confusión sobre la autoría del *hackeo* al comité demócrata.

La controversia sobre el origen de la infiltración no fue un obstáculo para que el contenido de los documentos filtrados siguiese alimentando la controversia electoral. El candidato republicano y los medios afines a su campaña no dudaron en seguir recurriendo a estas revelaciones para lanzar ataques sobre la honestidad de Hillary. El propio Donald Trump declararía en un mitin electoral: «Amo Wikileaks»[12], sin importarle demasiado cómo habían llegado esos documentos al portal del polémico Julian Assange.

La tecnología permitió a Rusia influir en la campaña de manera rápida, y a una escala sin precedentes. Sin embargo, la ejecución de la operación dejó numerosas pistas[13] que permitieron establecer una sólida atribución de responsabilidad hacia el Estado ruso. Con posterioridad a las elecciones, el Gobierno estadounidense desclasificaría una valoración conjunta de las diferentes agencias de inteligencia del país donde se afirmaba: «Evaluamos que Moscú aplicará las lecciones aprendidas de su campaña dirigida a las elecciones presidenciales de Estados Unidos a futuros esfuerzos de influencia en Estados Unidos y en todo el mundo, incluso contra los aliados estadounidenses y sus procesos electorales […] las opiniones públicas de Putin sobre las revelaciones sugieren que el Kremlin y los servicios de inteligencia seguirán considerando el uso de operaciones de filtración a través del ciberespacio debido a su creencia de que estas pueden lograr objetivos rusos con relativa facilidad sin un daño significativo a los intereses rusos»[14].

---

[11] RID, Thomas. «All Signs Point to Russia Being Behind the DNC Hack». *Motherboard,* July 25, 2016, disponible en https://motherboard.vice.com/en_us/article/all-signs-point-to-russia-being-behind-the-dnc-hack. Fecha de la consulta 02/06/2017.

[12] Vídeo de las declaraciones disponible en https://www.youtube.com/watch?v=mUtT0b0EnSw. Fecha de la consulta 02/06/2017.

[13] MANDIA, Kevin. *Disinformation: A Primer in Russian Active Measures and Influence Campaigns*. Prepared Statement before the United States Senate Select Committee on Intelligence, March 30, 2017, disponible en https://www.intelligence.senate.gov/sites/default/files/documents/os-kmandia-033017.pdf. Fecha de la consulta 02/06/2017.

[14] ODNI. «Assessing Russian Activities and Intentions in Recent US Elections: The Analytic Process and Cyber Incident Attribution». *Intelligence Community Assessment*, January 6, 2017, disponible en https://www.dni.gov/files/documents/ICA_2017_01.pdf. Fecha de la consulta 02/06/2017.

Francia: el alumno aventajado

Las elecciones presidenciales de 2017 tenían *a priori* los ingredientes necesarios para convertirse en otro ejemplo exitoso de una operación de influencia rusa: una elevada volatilidad electoral alimentada por la crisis de los partidos tradicionales, una creciente brecha social en torno a las cuestiones migratorias y el rol del islam en la sociedad francesa, y sobre todo: la existencia de un partido político con opciones reales, el Frente Nacional, alienado con algunos de los objetivos de la política exterior rusa, como la ruptura de la Unión Europea y el cuestionamiento de la existencia de la OTAN. Sin embargo, el caso francés se ha convertido en el ejemplo opuesto: aquel que describe las limitaciones de ese tipo de operaciones. El principal elemento diferenciador se haya precisamente en la existencia de un precedente, cuyas lecciones fueron interiorizadas por las potenciales víctimas.

Mientras que la ingenuidad del personal demócrata hizo posible la captura de sus contraseñas a través del envío de simples correos electrónicos fraudulentos, en el caso de sus equivalentes franceses no solo eran conscientes de que podían recibir este tipo de trampas, sino que las esperaban y trazaron un plan para cuando llegase ese momento[15]. Adoptar una actitud únicamente reactiva podía resultar contraproducente, ya que un rechazo continuado de los intentos rusos de captura de contraseñas terminaría derivando en una mayor agresividad y sofisticación de los *hackers* rusos, en cuyo caso, la infiltración podría pasar inadvertida. La contramedida consistió en hacer creer a los intrusos que habían alcanzado fácilmente su objetivo y se centrasen en la explotación de la información capturada. Para ello, crearon cuentas de correos específicas para ser posteriormente «sacrificadas». Las mismas fueron llenadas de documentos reales procedentes de la campaña de *En Marche!*, pero también de otra serie de archivos con información «fabricada». En el caso de los documentos reales, se seleccionó una amplísima muestra de materiales anodinos, pero relacionados con contenidos potencialmente útiles para una campaña de desprestigio (como, por ejemplo, facturas y otra información fiscal), lo que obligaría a los agentes rusos a dedicar gran parte de su tiempo a estudiar el detalle de esta montaña de información, en la búsqueda del dato que permitiese el *kompromat*. El objetivo perseguido era contaminar la credibilidad de cualquier filtración de documentos, incluyendo aquella

[15] NOSSITER, Adam *et al.* «Hackers Came, but the French Were Prepared». *The Ne York Times,* May 9, 2017, disponible en https://www.nytimes.com/2017/05/09/world/europe/hackers-came-but-the-french-were-prepared.html?_r=1. Fecha de la consulta 02/06/2017.

información que pudiese haber sido capturada sin conocimiento de los responsables de campaña. El impacto de cualquier dato quedaría atenuado si se lanzaba una duda razonable sobre su credibilidad, basándose en el señalamiento del carácter claramente fraudulento de algunos documentos, en los que podía encontrarse membretes y seños inexistentes, o habían sido editados para añadir metadatos que apuntaban directamente a los órganos de inteligencia rusa. Ante la opinión pública, cualquier filtración terminaría siendo percibida como la burda fabricación de un actor con intereses espurios[16].

Aunque, por el momento, no existe certeza sobre si la elección del momento estuvo determinada por las acciones del equipo de Enmanuel Macron destinadas a malgastar el tiempo de los intrusos digitales, lo cierto es que la filtración masiva de documentación no se produjo hasta el viernes 5 de mayo de 2017, a tan solo una hora de la finalización oficial de la campaña electoral y dos días antes de la celebración de las elecciones. Lo que si conocemos es cómo el equipo de Macron se encargó de preparar a la opinión pública para la inminente filtración de datos de la campaña. Para ello comunicó a varios medios de comunicación que la campaña había sido víctima de varios ciberataques lanzados por *hacker* vinculados a Rusia[17], aportando para ello un informe[18] que vinculaba este intento de penetración con otras operaciones previas de la inteligencia rusa, entre ellas el *hackeo* de las elecciones estadounidenses. Por otro lado, anunció la decisión de la campaña de no permitir[19] la cobertura de sus actos por parte de los dos medios de comunicación internacionales vinculados al Estado ruso: la cadena de televisión RT y la agencia de noticias Sputnik.

Bajo el hashtag *#MacronLeaks* se difundieron a través de redes sociales y en el portal Wikileaks los enlaces para la descarga de una carpeta con un peso de casi 9 gigas de datos. Una cantidad abrumadora de información cuya digestión no solo era inviable

[16] EVRON, Gadi. «Analyzing a counter intelligence cyber operation: How Macron just changed cyber security forever». *Hackernoon,* May 8, 2017, disponible en https://hackernoon.com/analyzing-a-counter-intelligence-cyber-operation-how-macron-just-changed-cyber-security-forever-22553abb038b. Fecha de la consulta 02/06/2017.

[17] SEIBT, Sebastian. «Cyber experts '99% sure' Russian hackers are targeting Macron». *France 24*, April 27, 2017, disponible en http://www.france24.com/en/20170426-france-macron-cyber-security-russia-presidential-campaign. Fecha de la consulta 02/06/2017.

[18] HACQUEBORD, Feike. «Two Years of Pawn Storm Examining an Increasingly Relevant Threat». *TrendLabs Research Paper* 2017, disponible en https://documents.trendmicro.com/assets/wp/wp-two-years-of-pawn-storm.pdf. Fecha de la consulta 02/06/2017.

[19] THE GUARDIAN. «Emmanuel Macron's campaign team bans Russian news outlets from events». *The Guardian,* April 27, 2017, disponible en https://www.theguardian.com/world/2017/apr/27/russia-emmanuel-macron-banned-news-outlets-discrimination. Fecha de la consulta 02/06/2017.

para un ciudadano medio, sino también para los principales medios de comunicación, los cuales carecían de los recursos humanos necesarios para escudriñar en unas pocas horas miles de documentos. Las limitaciones materiales, junto con la prohibición expresa[20] de la autoridad electoral de publicar o compartir contenido relacionado con la filtración, desactivaron las posibilidades de que esa avalancha de datos terminase traducida en titulares en medios de comunicación o *tweets* en redes sociales. Fuera de los circuitos mayoritarios, la difusión de las noticias procedentes de esa filtración sería marginal. Su ubicación en espacios burdamente conspiranoicos[21] restó impacto a los nuevos datos, al igual que había sucedido con otras *fake news* que días atrás se habían publicado contra el candidato francés[22].

El equipo de Macron no solo neutralizó la operación de influencia rusa, sino que resultó beneficiado al ser percibido por la opinión pública como la víctima de un intento intolerable de manipulación por un país extranjero que buscaba la victoria de su adversaria Marie Le Pen.

El futuro de las operaciones de influencia

Las elecciones presidenciales en Estados Unidos (2016) y Francia (2017) son ejemplos paradigmáticos del poder y las limitaciones de las operaciones de influencia en el ciberespacio. En ambos casos pueden extraerse una serie de lecciones sobre cómo evolucionarán este de tipo de injerencias en un futuro inmediato:

a) *La existencia de una fractura social es un prerrequisito para que la manipulación surja efecto*. Una elevada polarización sobre cuestiones centrales en la pugna electoral hace posible que los diferentes actores estén dispuestos a rentabilizar la información perjudicial del oponente, con independencia de su origen ilícito, carácter fraudulento o implicaciones morales. Su utilización explícita por parte de algún candidato le otorga una relevancia que multiplica su impacto en la opinión pública.

[20] WILLSHER, Kim. «French media warned not to publish Emmanuel Macron leaks». *The Guardian,* May 6, 2017, disponible en https://www.theguardian.com/world/2017/may/06/french-warned-not-to-publish-emmanuel-macron-leaks. Fecha de la consulta 02/06/2017.
[21] HERRWOLF. «Documentos filtrados de Macron contienen planes secretos para la islamización de Francia y Europa». *The Daily Stormer*, 6 de mayo de 2017, disponible en http://es.dailystormer.com/2017/05/06/documentos-filtrados-de-macron-contienen-planes-secretos-para-la-islamizacion-de-francia-y-europa/. Fecha de la consulta 02/06/2017.
[22] GRODIRA, Fermin. «Macron, el protegido de Al Qaeda que se lava las manos tras saludar obreros y se acuesta con su hijastra». *Magnet,* 3 de mayo de 2017, disponible en https://magnet.xataka.com/en-diez-minutos/macron-el-protegido-de-al-qaeda-que-se-lava-las-manos-tras-saludar-obreros-y-se-acuesta-con-su-hijastra. Fecha de la consulta 02/06/2017.

La impulsiva personalidad de Donald Trump no solo fue decisiva para situar las filtraciones en el centro de la agenda política, arrastrando a la campaña demócrata a una postura defensiva. También limitó las posibilidades de que el Gobierno de los Estados Unidos pudiese adoptar represalias más ambiciosas[23], debido al temor de que el candidato republicano las deslegitimase presentándolas como un intento del presidente Obama de entrar en campaña a favor de su rival. Por el contrario, Marie Le Pen fue mucho más comedida a la hora de utilizar este tipo de material, lo que permitió que Enmanuel Macron pudiese recontextualizar el asunto de las filtraciones desde una perspectiva ventajosa.

b) *Lo que funciona una vez no tiene porqué seguir haciéndolo*. El inesperado desenlace de las elecciones estadounidenses actuó como un revulsivo en la campaña francesa. El equipo de Macron estaba convencido de que sería objeto de un ataque idéntico, lo que les llevó a diseñar una respuesta activa. Por el contrario, cuando se dirigieron hacia el escenario francés, los *hackers* rusos no modificaron ni los objetivos, ni los procedimientos operativos, lo que hizo que su manipulación fuese ineficaz frente a una víctima prevenida y preparada. El fracaso francés empujará a la inteligencia rusa a adoptar formas novedosas de aproximarse a los procedimientos electorales sobre los que desea influir, lo que abre un amplio abanico de innovaciones sobre las que se empieza a especular: el uso impostado de los perfiles de los candidatos en redes sociales para introducir información que desestabilice la campaña, ciberataques destinados a sabotear el proceso de recuento de votos para dar argumentos a los candidatos que desean poner en duda la limpieza del proceso, etc.

c) *El orden los factores altera el producto.* Cualquier actor interesado en manipular las corrientes de opinión pública debe resolver previamente el dilema sobre cuál es el momento idóneo para actuar. ¿Es más efectivo actuar en el largo plazo o inmediatamente antes de que se produzcan las votaciones? Existen precedentes y argumentos empíricos que respaldan una y otra alternativa, lo que obliga el manipulador a actuar como un aprendiz de brujo incapaz de dominar y predecir los efectos de sus acciones. En el caso americano y francés vemos ejemplos de una actuación prolongada y de una irrupción en el último momento. En teoría existen

[23] LIPTON, Eric *et al*. «The Perfect Weapon: How Russian Cyberpower Invaded the U.S.». *The New York Times,* December 13, 2016, disponible en https://www.nytimes.com/2016/12/13/us/politics/russia-hack-election-dnc.html. Fecha de la consulta 02/06/2017.

más probabilidades de que el electorado modifique sus percepciones y preferencias a través de una sucesión sostenida de impactos informativos, pero este enfoque también permite que el resto de actores se adapten y puedan poner en marcha acciones que neutralicen el efecto de la «desinformación». Introducir la intoxicación de manera inmediatamente anterior a las elecciones impide que las víctimas puedan articular una respuesta, pero dificulta que el electorado pueda digerir la nueva información en tan corto espacio de tiempo. En este sentido, cada país es un caso único que exige una aproximación específica acorde a sus riesgos y oportunidades.

*Manuel R. Torres Soriano**
Profesor Titular de Ciencia Política,
Universidad Pablo de Olavide, Sevilla
Miembro Grupo de Estudios Seguridad Internacional (GESI)