FACULTAD DE CIENCIAS HUMANAS Y SOCIALES

LA MANIPULACIÓN RUSA EN LOS MEDIOS DE COMUNICACIÓN

Autor: María Burgos Torrado

Tutor: José María Marco Tobarra

5º E5

Ideas Políticas y Relaciones Internacionales

Madrid, 2019

A mi padre, fiel defensor de la verdad,
por inculcarme este prudente escepticismo.

TABLA DE CONTENIDO

Resumen

El fin de la Guerra Fría ha dado paso a una guerra cibernética, protagonizada por el uso de las nuevas tecnologías y los medios de comunicación como instrumentos de influencia que sirven a unos intereses, en muchas ocasiones, ocultos. Esto les convierte en armas poderosas capaces de influir en decisiones cruciales en el panorama internacional. Desde sus inicios como espía, Putin ha establecido la manipulación de masas y la desinformación como uno de los pilares subyacentes de su gobierno. Este trabajo de fin de grado tiene como objeto el análisis de los medios de manipulación que Rusia utiliza para consolidar su presencia internacional y de su aplicación práctica.

Palabras clave

Rusia, medios de comunicación, manipulación, Vladimir Putin, desinformación.

Abstract

Even though it seems like the Cold War is over, a ciberwar has been set up, in which media plays an important role in terms of influence and manipulation. Technologies have become dangerous weapons that are able to spread any idea that benefits certain interests beyond them. Putin started serving Russia as a spy. That is why he knows perfectly how to place manipulation and disinformation as an elemental factor of its government. This Project is going to focus on the study of the means that Russia uses to manipulate society and governments all over the World, to make international politics work in order to comply Russian interests.

Key Words

Russia, manipulation, media, Putin, disinformation.

Abreviaturas

APT: Advanced Persistent Threat (Amenaza Persistente Avanzada)

BTB: Vneshtorg Bank

CCDF: Complementary Cumulative Distribution (Función de distribución acumulada)

EEUU: Estados Unidos

FBI: Federal Bureau of Investigation

FSB: Federal Security Service (Servicio de Seguridad Federal)

GRU: Main Intelligence Directorate

IRA: Internet Research Agency (Agencia de Investigación de Internet)

KGB: Komitet Gosudarstrennoaja Bezopasnosty (Comité de la Seguridad del Estado)

LLC: Limited Liability Company

RPV: Red Privada Virtual

RT: Russia Today

UE: Unión Europea

URL: Uniform Resource Locator (Localizador de Recursos Uniforme)

URSS: Unión de Repúblicas Socialistas Soviéticas

USA: United States of America

VEB: Vnesheconom Bank

CAPÍTULO 1: INTRODUCCIÓN

"For years, Vladimir Putin's government has engaged in a relentless assault to undermine democracy and the rule of law in Europe and the United States. Mr. Putin's Kremlin employs an asymmetric arsenal that includes military invasions, cyberattacks, disinformation, support for fringe political groups, and the weaponization of energy resources, organized crime, and corruption. The Kremlin has refined the use of these tools over time and these attacks have intensified in scale and complexity across Europe. If the United States fails to work with urgency to address this complex and growing threat, the regime in Moscow will become further emboldened. It will continue to develop and re- fine its arsenal to use on democracies around the world, including against U.S. elections in 2018 and 2020".

United States Senate, Committee On Foreign Relations,

Washington, DC, January 10, 2018

1.1 Estado de la cuestión

La aparición de los medios de comunicación en masa es uno de los cambios más importantes que ha experimentado el último medio siglo. Dicho acontecimiento ha supuesto una alteración del orden internacional y del concepto tradicional de guerra. La sociedad está inmersa en un mundo hipermediatizado, en el que los medios de comunicación tratan de dar una falsa imagen de neutralidad que, en la mayoría de los casos, carece de tal imparcialidad. La gravedad del asunto reside en que la información juega un papel importante en la manera de percibir la realidad y, dependiendo de con qué fines sea empleada, puede desembocar en unos resultados u otros (Wolton, 1992, p.10).

Las Relaciones Internacionales están formadas por la coexistencia de distintas potencias, cada una con un grado de capacidad de influencia. De hecho, hay autores que clasifican a los distintos sujetos que conforman el panorama internacional en dominadores o dominados (Baños, 2017, p.21). Los clásicos generadores de poder, como la influencia militar y económica, han dado paso a la creciente relevancia de la influencia tecnológica y cultural, ambas ligadas entre sí. No obstante, el objetivo sigue siendo el mismo: la pugna por el poder, siendo las tres obsesiones actuales los recursos naturales, la energía y la tecnología (Baños, 2017, p.39).

Fukuyama consideró la caída de la Unión Soviética como el "fin de la historia". Para este autor, el progreso humano había llegado a su fin a finales del siglo XX (Fukuyama, 1992). Sin embargo, ni siquiera habían pasado 10 años cuando procedió a reconsiderar algunos puntos de su obra, admitiendo que el curso que tomara la evolución de las tecnologías podía alterar su teoría de una historia direccional y programática. En palabras de este autor: "La mundialización actual está respaldada por la revolución en la tecnología de la información"(Fukuyama, 1999).

Por su parte, autores como Huntington consideraron que la historia no podía tener fin, sino que experimentaría un reajuste a raíz del desmoronamiento del sistema bipolar de la Guerra Fría, responsable de dividir el mundo en dos bloques. Por consiguiente, la violencia entre los Estados occidentales y no occidentales aumentaría, fruto de una coexistencia de eterna tensión (Huntington, 1997). Ambos autores acertaron en parte. En primer lugar, es cierto que el curso de las dos últimas décadas ha sido protagonizado por la evolución de las tecnologías. Sin embargo, el reajuste al que se refería Huntington se ha materializado en las Relaciones Internacionales con el surgimiento de nuevas modalidades bélicas, predominando la guerra cibernética por encima de la violenta guerra física, siendo la primera menos costosa pero igual de peligrosa que la modalidad tradicional. Este nueva tipología de guerra se diferencia de la anterior tanto en la clase de armas empleadas como en la finalidad de la misma, que se basa en ganar influencia en lugar de ganar territorios (Milosevich-Juaristi, 2017). Pedro Baños define a la tradicional figura del espía como "las extensiones de los Estados que disimulan en los países enemigos, o incluso aliados, con el fin de obtener información beneficiosa para los intereses del Estado a cuyas órdenes trabajan" (Baños, 2017, p.145). No obstante, estas personas físicas han sido sustituidas por personas virtuales, como tendremos ocasión de ver a lo largo de este trabajo.

Rusia ha asumido este cambio en las tendencias bélicas. Durante el año 2017, EEUU encabezó la lista de Estados que más habían invertido en su presupuesto militar, seguido por China, Arabia Saudí, Reino Unido, India, Japón y Francia. Rusia ostenta la octava posición en este ranking, dedicando tan solo un 1,9% del PIB (International Institute for Strategis Studies, 2017). Además, se sitúa como el segundo país del mundo en el ranking de mayores exportadores de armamento, mientras que, en el mismo ramo, ni siquiera figura entre los 10 primeros puestos del ranking de mayores importadores (SIPRI, 2018). A pesar de que las cifras a las que nos estamos refiriendo no son

precisamente bajas, el Kremlin es consciente de que una de las armas más peligrosas en el ejercicio de la guerra es aquella que permita gobernar al intelecto y los sentimientos humanos, llámese propaganda de guerra, desinformación o *fake news*. Es por ello que propaganda y guerra han ido siempre de la mano, si bien es cierto que el papel que juegan los medios de comunicación actualmente es mucho mayor que el que jugaban anteriormente (Contreras, 2004, pp.17-18). Rusia ha sido acusada de emplear estos medios para alcanzar una dominación indirecta, que se extiende más allá de sus fronteras y opera a través de la apropiación de la cultura. Conseguir captar la opinión pública es el primer paso para dominarla, consolidando una sociedad polarizada y desconfiada (Singer, 2018, p.208).

Asimismo, las noticias de contenido sensacionalista tienen la finalidad de favorecer a la dominación a través del miedo. Mediante esta estrategia, Rusia consigue que los Estados que se sienten vulnerables inviertan en armas, factor beneficioso para la economía rusa, pues, como ha sido mencionado anteriormente, Rusia es el segundo país del mundo que más armas exporta (Baños, 2017, p.171).

El tipo de guerra que está desarrollando Rusia, se identifica con el término *kombinaciya*[1], definido como un tipo de operación que integra diferentes instrumentos propios de la guerra de la información: ciberguerra, ciberinteligencia, desinformación y propaganda con el fin de quebrar los valores de la democracia liberal (Milosevich-Juaristi, 2017).

Actualmente, se están desarrollando diversas investigaciones para probar la interferencia rusa en casos como, entre otros, el proceso del *Brexit*, las elecciones presidenciales de Estados Unidos de 2016, las elecciones francesas de 2017 y en la celebración del referéndum ilegal de Cataluña de ese mismo año. Respecto a este último supuesto, las investigaciones desarrolladas han demostrado importantes contradicciones entre las afirmaciones realizadas por miembros del Kremlin como Yuri Korchagin, embajador de Rusia en España, Serguéi Lavrov, Ministro de Asuntos Exteriores de Rusia, y el propio presidente del gobierno ruso Vladimir Putin; y los mensajes divulgados por los medios de comunicación rusos, financiados por el Kremlin. Durante el mes de septiembre del 2017, las publicaciones relacionadas por dichos medios rusos acerca de Cataluña incrementaron en un 2.000%. El contenido de las noticias

[1] Término ruso que quiere decir combinación

provenientes de estos medios rusos se centraron en destacar las debilidades y problemas internos de España, democracia occidental. Asimismo, un estudio realizado por el Real Instituto Elcano, destacó como finalidad de la injerencia rusa en el referéndum ilegal de Cataluña favorecer la división entre los ciudadanos españoles y la confrontación entre España y el resto de Estados miembros de la UE, desacreditar a las instituciones europeas y crear confusión (Milosevich-Juaristi, 2017).

Por lo tanto, el Kremlin es un actor participante activo en este tipo de guerra de información que encuadra en la categoría de guerra híbrida, mencionadas en el siguiente apartado. El escenario puede variar de un estado a otro. No obstante, los intereses rusos no han cambiado desde la caída de la URSS, pudiendo ser resumidos en dos: desacreditar el orden liberal occidental y distraer la atención de los ciudadanos rusos de los problemas internos.

1.2 Marco teórico

Las distintas tradiciones de pensamiento que han predominado en el estudio de las Relaciones Internacionales, pueden resumirse en cuatro teorías: el realismo, el liberalismo, el marxismo y el constructivismo (Pauselli, 2013). Para comprender el objeto de estudio de este trabajo, cabe prestar especial atención a las premisas del realismo. En efecto, a finales de la Guerra Fría, el paradigma realista reapareció con importante repercusión en el estudio de las Relaciones Internacionales, etapa protagonizada por la complementariedad entre los distintos paradigmas (Barbé, 1987). Sin embargo, coincidimos con Robert Keohane en que el realismo es el núcleo a partir del cual han progresado las distintas relaciones entre los diversos actores que forman parte del panorama internacional. Citando a este autor: "El realismo es un componente necesario en cualquier análisis coherente de la política mundial porque la atención que presta al poder, a los intereses y a la racionalidad es crucial para comprender el tema" (Keohane, 1983, p.504).

Hans Morgenthau definió el realismo como la teoría que explica la realidad internacional en función del interés intrínseco de los Estados de asegurar su supervivencia. Para ello, el Estado busca consolidar su poder con el fin de alcanzar la dominación de otras naciones (Morgenthau, 1986, pp.19-20). Por ende, pueden localizarse tres postulados fundamentales en este paradigma: estatocentrismo, naturaleza conflictiva de las relaciones entre Estados y centralidad del poder.

El realismo se clasifica como un paradigma estatocéntrico, pues sitúa al Estado como actor protagonista de las Relaciones Internacionales. En una primera aproximación, podría parecer que este trabajo no encaja en esta categoría, pues se resaltan las acciones desarrolladas por diversos sujetos no estatales que han sido de gran relevancia para el curso de este estudio, por ejemplo WikiLeaks. No obstante, el objeto del presente análisis no es el funcionamiento de los medios de comunicación ni el papel que juegan en el panorama internacional. En realidad se están analizando los intereses de un Estado en concreto, Rusia; y qué medios está empleando para llevarlos a cabo. Se trata de un país con ansia de dominación, cuyas pretensiones parecen irreconciliables con Occidente, por lo que este trabajo fundamenta la visión pesimista de que las Relaciones Internacionales están protagonizadas por un constante estado de tensión interestatal. Se trata de un Estado (Rusia) atacando mediante medios cibernéticos a otros Estados. Esta afirmación se ve reforzada con las constantes denuncias a tales acciones por parte de los distintos Estados que han sido objeto de este ataque.

Es en este punto donde procede hacer una aclaración, relativa al concepto de guerra híbrida, desarrollada, entre otros, por Rusia. Esta modalidad admite como participantes de la guerra híbrida tanto a actores estatales como no estatales. Si bien es cierto que en este caso de estudio el protagonista es un Estado, Rusia utiliza tácticas novedosas que hacen que la amenaza física haya tenido que dar paso a otro tipo de ataques. En palabras de Frank Hoffman: "las doctrinas militares convencionales del siglo XX de la era industrial (…) están efectivamente muertas" (Hoffman, 2007, p.43). Esta nueva modalidad de guerra híbrida se diferencia del estilo bélico convencional, fundamentalmente, en las modalidades de los medios empleados. Los participantes en las guerras híbridas emplean tanto armas y misiles, como sistemas de comando encriptados o ciberataques, combinando las tácticas convencionales con nuevas estrategias irregulares y, asimismo, actos terroristas. La difusión de la tecnología militar avanzada hace que este tipo de guerras sea aún más letal que la modalidad convencional, gracias al empleo de los medios de comunicación como captadores de opinión pública (Hoffman, 2007, pp.14-16). Otros autores precisan que la diferencia entre la guerra híbrida y un mero acto criminal es que en ésta el actor participante ha de perseguir el fin político de imponer su voluntad e intereses (Eissa, 2011, p.13).

Retomando el análisis del realismo, Morgenthau explica que los Estados se mueven en busca de su interés nacional, promovido por su política exterior (Morgenthau, 1986,

p.16). El presupuesto ruso dedicado a la proliferación de los medios de comunicación prorrusos, así como la extensión de los mismos por todo el mundo, se debe a que el Kremlin emplea tales medios como instrumentos fundamentales de su política exterior. Como ha sido explicado en el apartado anterior, Rusia no es precisamente el Estado del mundo que dedica un mayor porcentaje de su PIB al presupuesto militar. El motivo de ello es que Rusia es uno de los mayores exponentes de actor participante en la guerra híbrida, y su manera de defender el interés nacional es difundiendo su percepción de la realidad a través de estos nuevos mecanismos de política exterior.

La segunda premisa que constituye la teoría realista de Morgenthau es la visión anárquica de las relaciones internacionales, en constante conflicto debido a la pluralidad de actores y el antagonismo entre ellos, lo que lleva a su vez a este autor a encuadrar su teoría en una concepción maquiavélica y hobbesiana, debido a que considera que los actores internacionales se encuentran en el estado de naturaleza (Morgenthau, 1986, p.234). Asimismo, la teoría realista comparte con la filosofía de Hobbes el hecho de que el hombre, o en este caso el Estado, se encuentre constantemente en un estado de búsqueda de poder. Asimismo, Maquiavelo y Hobbes coincidieron en que a dicha ansia se añade el afán de seguridad. Para Hobbes, los hombres son naturalmente enemigos, debido a que los recursos naturales necesarios para la supervivencia son escasos y eso hace que estén en constante lucha entre ellos. Es por ello que los hombres están inmersos en una guerra de todos contra todos mientras permanezcan en el estado de naturaleza (Hobbes, 2006). Precisamente este postulado es la base de la ramificación de esta teoría, conocida como realismo clásico. Según Waltz, el motivo de que los Estados compitan continuamente entre ellos reside en la naturaleza humana, pues la conducta de los hombres está condicionada por su interés y el ansia de seguridad y poder. Consecuentemente, como el Estado se encuentra compuesto por seres humanos, las Relaciones Internacionales quedan configuradas por conductas egoístas por parte de dichos actores estatales (Waltz, 1959, pp.26-27). Otra rama del realismo, el realismo estructural, considera que el motivo de dicha actitud reside en la anarquía persistente en el panorama internacional y no en la naturaleza humana (Pauselli, 2013).

La tercera premisa para Morgenthau es la centralidad del poder. Este autor considera que la obtención de poder es el objetivo principal de la política exterior de los Estados (Barbé, 1987). Como será explicado a lo largo de este trabajo, la infraestructura de medios de comunicación desarrollada por Rusia durante las últimas décadas no tiene

otra finalidad que consolidar su presencia internacional. Para ello, la manera de fortificar su poder es adquiriendo zonas de influencia. El objetivo de la política exterior rusa es devolver a Rusia el *estatus* de gran potencia. Sin embargo, sus ansias de poder se traducen en ganar influencia, no territorios, rasgo que, tal y como ha sido mencionado, caracteriza a la guerra híbrida.

1.3 Marco temporal

En 1990, la URSS se encontraba en una situación de crisis interna que desembocó en su disolución. Desde el 11 de marzo de dicho año hasta el 25 de diciembre del año siguiente, se materializó la independencia de 15 Repúblicas de la Unión soviética. El presidente que tuvo que hacer frente a este proceso fue Mijaíl Gorbachov, sucedido en 1991 por Boris Yeltsin (Murillo, 2005). No obstante, en 1999, la candidatura de este último estaba más que acabada, y era el momento de encontrar a alguien de confianza (Pizzonia, 2018, p.29). Fue entonces cuando la carrera de Vladimir Putin despegó, ganando las elecciones en el año 2000. Su carrera política se ha prolongado hasta la actualidad, con tan solo una interrupción en la legislatura del 2008 al 2012 (Lieven, 1999).

Respecto al marco temporal de los servicios de inteligencia rusos, en el año 1923 se fundó el KGB, bajo la presidencia de Iósif Stalin. Durante la Guerra Fría, este organismo desarrolló unas 10.000 operaciones basadas en la desinformación (Singer, 2018, p.103). No obstante, la disolución de la URSS y de dicho organismo tan solo dista de unas semanas. El sucesor del KGB es el FSK, fundado en 1992, pronto transformado en el FSB, que ha desarrollado su labor desde el año 1995 hasta la actualidad. La estrecha relación entre el actual presidente ruso y los servicios de inteligencia se debe a que el propio Vladimir Putin formó parte del KGB desde el año 1975 hasta que fue nombrado Primer Ministro por Boris Yeltsin en el año 1999, siendo el director de dicho organismo a las puertas de las elecciones que supondrían su acceso al poder como presidente del Gobierno (Bennet, 2000).

Debido a la constante evolución de los medios de comunicación, este trabajo emplea como marco temporal el intervalo de tiempo que se extiende desde la llegada de Putin al poder, en el año 1999, hasta la actualidad, haciendo especial incidencia en los años que discurren desde 2014 hasta 2016 durante el análisis del caso estudio seleccionado.

1.4 Marco geográfico

En relación con el marco geográfico, acotamos este trabajo al Estado ruso como ente centralizador de los medios de manipulación objeto de estudio, así como a los Estados que hayan sido alcanzados por los medios de manipulación rusa, con especial referencia a Estados Unidos.

1.5 Preguntas de investigación y objetivos

En base a las reiteradas denuncias llevadas a cabo por distintos actores internacionales, en referencia a las supuestas técnicas de manipulación desarrolladas por Rusia, cabe preguntarse cuáles son los medios que el gobierno ruso tiene a su disposición, así como el funcionamiento del operativo empleado para influenciar la política internacional. Asimismo, ¿cuáles son los verdaderos objetivos del Kremlin? Para comprender esta última cuestión es necesario cuestionarse cómo fue el ascenso de Putin al poder. ¿Es cierto que anteriormente fue un espía del KGB?

Para responder a dichas cuestiones, será analizado un caso de estudio relativo a la presencia rusa durante todo las elecciones presidenciales de Estados Unidos del año 2016. ¿Qué era lo que más le interesaba a Putin? ¿Qué estrategias fueron llevadas a cabo? ¿Tuvo el gobierno ruso algo que ver con la filtración de los emails de Hillary Clinton por parte de WikiLeaks?

Por lo tanto, este trabajo se centrará en responder a los interrogantes que envuelven la llegada de Putin al gobierno, cómo fue centralizando todos los servicios de inteligencia en su persona, cómo han evolucionado los medios de manipulación y cómo podría ejemplarizarse su aplicación práctica, mediante el mencionado caso de estudio. Para resolver a estas cuestiones, serán analizados los términos de *fake news*, diplomacia pública, desinformación y propaganda computacional.

1.6 Motivaciones

Joseph Goebbels, ministro para la Ilustración Pública y Propaganda durante el Tercer Reich, popularizó la frase “una mentira repetida muchas veces se convierte en una gran verdad”. Sin embargo, el origen de dicha cita se remonta a 1917, perteneciendo a Lenin (Baños, 2017, p.245). Hace más de un siglo que Rusia no contempla un régimen político sin la presencia del poder persuasivo de la propaganda. No obstante, este

trabajo coincide con George Orwell en que "en una época de engaño universal, decir la verdad se convierte en un acto revolucionario" (Marcus, 1982).

Por lo tanto, las motivaciones que han llevado al desarrollo de este estudio son el interés por conocer más a fondo el funcionamiento político de una de las mayores potencias mundiales, como es Rusia; sus mecanismos de control, dentro y fuera de las fronteras; los intereses perseguidos por el Kremlin y el papel que juegan a día de hoy las redes sociales en nuestra vida diaria, así como la manera en la que nuestras propias decisiones pueden estar influenciadas por una persona, física o virtual, operando con un ordenador desde la otra punta del planeta.

1.7 Metodología

Con el objetivo de probar la hipótesis previamente planteada y de responder a las preguntas de investigación enunciadas, se ha recurrido a la técnica de investigación, consistente en la recopilación y análisis de la información proporcionada por diversas fuentes, clasificadas en primarias y secundarias.

a) Fuentes primarias. Cabe incluir en esta categoría el empleo de dos documentos elaborados por el propio Gobierno de Estados Unidos: Una denuncia interpuesta por el fiscal Robert Swan Mueller ante la Corte del Distrito de Columbia y un documento elaborado por el Comité de Asuntos Exteriores del Senado, alarmando de la injerencia rusa en las pasadas elecciones y acusando a Donald Trump de no intentar frenar los ciberataques.

b) Fuentes secundarias:

- Obras literarias: con el objetivo de desarrollar el análisis que ocupa el capítulo II de este trabajo, se ha recurrido a la lectura y síntesis de obras publicadas por autores bien conocidos en el estudio de esta materia, destacando las obras de Peter Singer, Clinton Watts y Pedro Baños. Las obras citadas analizan desde distintas perspectivas la hipótesis de este trabajo. El motivo de su utilidad es que los distintos autores de dichas obras escriben acerca de su experiencia profesional en diversos servicios de inteligencia. Singer fue el coordinador del Defense Policy Task Force durante el gobierno de Barack Obama. Además de su trabajo en temas de conflicto, Singer es miembro del Comité Asesor del Departamento de Estado sobre Política Internacional de

Comunicaciones e Información y actualmente es miembro del State Department's Advisory Committee on International Communications and Information Policy. Asimismo, Clinton Watts es miembro del Center for Cyber and Homeland Security de la Universidad de Washington, tras haber formado parte de la Armada estadounidense, agente del FBI. Ambos autores estudian en sus obras, con profundidad, la injerencia rusa en las elecciones americanas, por lo que han sido fundamentales para el análisis del caso de estudio. Por último, Pedro Baños, coronel del Ejército de Tierra y anterior jefe de Contrainteligencia y Seguridad del Cuerpo de Ejército Europeo de Estrasburgo explica conceptos geopolíticos cruciales para este trabajo, como la desinformación, las áreas de influencia en el mundo y las motivaciones perseguidas por los distintos Estados.

- El estudio de la manipulación rusa en los medios de comunicación ha sido objeto de numerosas publicaciones académicas, que han sido de gran utilidad para el desarrollo de este trabajo y para conocer a los principales autores que han estudiado esta materia. Dichas publicaciones académicas también han servido para localizar las obras de los filósofos más influyentes en la concepción realista de las relaciones Internacionales.
- Artículos periodísticos: En especial, han sido de gran utilidad las investigaciones realizadas por el New York Times y la BBC, que han realizado entrevistas a ex *trolls* rusos que cuentan de primera mano su experiencia. Asimismo, se han empleado algunos artículos de periódicos españoles, con el fin de retratar el impacto de esta guerra cibernética en la opinión pública.
- Informes de organismos internacionales. Frente a las conclusiones teóricas que se extraen del estudio de las fuentes previamente detalladas, estos informes han permitido analizar con detalle a través de datos económicos como, por ejemplo, el presupuesto ruso destinado a armamento. Estos documentos sirven para comprender el contexto económico, social y cultural en el que se desarrolla este conflicto. Asimismo, el recurso a estos informes nos permite visualizar con mayor precisión la entidad del conflicto, así como sus consecuencias, fundamentalmente sociológicas.

CAPÍTULO 2: LA MANIPULACIÓN RUSA EN LOS MEDIOS DE COMUNICACIÓN

2.1 Vladimir Putin, de espía a presidente del Gobierno

En 1999, el ex presidente ruso Boris Yeltsin tuvo que enfrentarse a la siguiente realidad: su segunda legislatura estaba a punto de finalizar y sus rivales políticos estaban decididos a hacerse con una Rusia descontenta, endeudada y sumergida en una profunda crisis económica. La precariedad económica se tradujo en una crisis de salud y mortalidad que causó al menos tres millones de muertes (English, 2017). Todo ello, sumado a las constantes acusaciones de corrupción hacia Yeltsin, hizo que el ex presidente comprendiera que necesitaba un sucesor que pudiera protegerlo a él y a su familia cuando dejara el cargo. Fue entonces cuando fijó su vista en Vladimir Putin, director del Servicio de Seguridad Federal (FSB), organismo sucesor del KGB (Singer, 2018, p.107), que había demostrado en determinadas ocasiones su lealtad a Yeltsin.

En 1999, el fiscal general del Estado ruso, Yury Skuratov, estaba llevando a cabo una investigación sobre la corrupción en el Kremlin, especialmente entre los miembros de la familia de Yeltsin. No obstante, tal operación se vio interrumpida cuando Skuratov fue llamado por el jefe de personal de Yeltsin para mostrarle una cinta de video en la que parecía que salía él mismo en una situación comprometida, con dos chicas de compañía en una habitación de un hotel. Skuratov no tardó en presentar su dimisión. Sin embargo, nunca reconoció ser él aquel hombre que aparecía en el video, afirmación que dio lugar a una nueva investigación por riesgo de que tal video fuera un montaje. Las repercusiones por no admitir que era él mismo el que salía en el video fueron su reproducción en una cadena de televisión rusa. He aquí los comienzos de la carrera política de Vladimir Putin, que no solo había entregado el video, sino que a continuación apareció en la televisión confirmando que la persona que aparecía era el propio fiscal (Ioffe, 2017).

Un ex general del KGB, Oleg Kalugin, sostiene que todo el episodio "fue una operación especial del FSB para desacreditar a un funcionario con la ayuda de un video en el que aparecía una persona que se parecía al fiscal general". En efecto, la operación funcionó. No solo supuso el cese de la investigación promovida por el fiscal general, sino que además Putin había probado su lealtad a Yeltsin. El siguiente paso que dio el ex presidente, fue proponer a Putin como Primer Ministro, candidatura aprobada por el

Parlamento Ruso. Putin aprovechó esta oportunidad, para mejorar su imagen y presencia pública, así como el número de potenciales votantes. Su manera de reaccionar ante los atentados de Chechenia favoreció a su ascenso al poder, dando la imagen de un político fuerte y comprometido. Sin embargo, los bombardeos de Chechenia no han estado exentos de polémica, al ser una operación que concluyó sin determinar la culpabilidad de ningún checheno concreto y, por supuesto, sin pruebas de que los terroristas chechenos fueran los responsables (Committee On Foreign Relations Of The USA, 2018, p.15). Una vez más, se trataba de una situación perfecta para propiciar el aumento de popularidad de Putin.

El proceso de ascenso al poder fue rápido. Boris Yeltsin dimitió el 31 de diciembre de 1999 y Putin ganó las siguientes elecciones tras el desarrollo de una breve campaña electoral, un aumento de su reciente popularidad gracias a la guerra de Chechenia y contando con un enorme apoyo económico procedente de oligarcas rusos interesados en que se consolidara su gobierno (Lieven, 1999). Curiosamente, lo primero que hizo al llegar al poder fue asegurar la inmunidad de Yeltsin frente a toda posible acusación de corrupción. Ambos políticos habían salido ganando. Proveniente de una familia humilde que apenas podía permitirse una habitación para vivir, Putin se había convertido en uno de los hombres más poderosos del mundo.

Eliminó los centros de poder independientes al redistribuir los recursos de los oligarcas a los oficiales de seguridad, absorbiendo los medios controlados por los oligarcas y neutralizando los centros de poder regionales que no respetaban las órdenes de Moscú. Comenzó a instalar a antiguos compañeros del FSB en posiciones de poder, de manera que en el año 2004, los ministerios más importantes estaban dirigidos por ellos. El poder ruso se estructuró como una jerarquía que situaba a Putin en la cúspide de la pirámide, pero cuyos escalones inferiores son de dudoso valor. Podría decirse que primero está la figura indiscutible de Putin y luego todos los demás grupos que compiten entre ellos por los recursos. Asimismo, desde su llegada al poder, se hizo con el control directo de la industria del gas y el control sobre los bancos rusos de la red troncal (VEB, VTB y Sberbank) (Minchenko Consulting Communication Group, 2016).

Los servicios de seguridad rusos se incrementaron de forma directamente proporcional al aumento de poder de Putin, consolidando una red de agencias de inteligencia que conducen no solo el espionaje, sino también las medidas activas

dirigidas a desestabilizar a los gobiernos occidentales con sistemas políticos basados en una democracia liberal, desarrollando operaciones en apoyo de los intereses económicos rusos y los ataques a todo enemigo político.

Sus aspiraciones pueden comprenderse con mayor claridad teniendo en cuenta sus antecedentes familiares y personales. Los historiadores coinciden en la concurrencia de dos factores como determinantes a la hora de marcar la carrera política del actual presidente del gobierno ruso. El padre de Vladimir Putin formó parte de la Flota Roja durante los años 30, además de durante la II Guerra Mundial, conocida por los rusos como "la Gran Guerra Patriótica", cuyo origen sitúan en la invasión alemana de 1941 de la Unión Soviética (Morales, 2003). Además de sus antecedentes familiares, el segundo factor a tener en cuenta, es que Putin vivió en primera fila cómo durante la Guerra Fría la propaganda soviética se hacía con cada rincón de la URSS, mostrando a los agentes de inteligencia como héroes que luchaban contra el invasor. Consecuentemente, no es de extrañar que Putin se sintiera atraído por el KGB desde muy joven, lo que le llevó a ingresar en la organización en 1975, nada más acabar sus estudios universitarios. En 1985 fue destinado a la República Democrática Alemana. Las funciones que desempeñó en esta misión no se conocen con exactitud. Sin embargo, existen indicios de que su traslado tuvo como motivo desarrollar tareas de reclutamiento y mediar entre los servicios de inteligencia soviéticos y germanos, palabras que parecen más políticamente correctas que el término "espía" (Bennet, 2000).

Cuando regresó a la URSS, se dedicó a movilizar toda una red de informadores que se encargaban de luchar contra cualquier persona, movimiento u opinión que contradijera al entonces gobierno soviético. El hecho de que Putin haya reconocido que se siente más que orgulloso de haber pertenecido al KGB, demuestra que está más que de acuerdo con las medidas represivas que esta organización implantó en la antigua URSS, logrando controlar cada sector de la sociedad, y de la economía, así como a la policía (Morales, 2003). No es de extrañar pues, que cuando Vladimir Putin se convirtió en presidente del gobierno concedería un papel privilegiado a los órganos de seguridad e inteligencia, incluso concentrando sus funciones, de nuevo, en una agencia que se asemeja al antiguo KGB, cuya disolución tuvo lugar en el año 1991, tan solo unas semanas antes de la disolución de la antigua URSS.

Actualmente, el FSB es la más poderosa de las agencias de inteligencia rusa, sucesora del antiguo KGB. No solo realiza, al menos, las mismas funciones, sino que

además cuenta con toda las documentación y archivos que recopiló el KGB. Su alcance se extiende desde la televisión hasta las universidades, bancos y ministerios. De esta forma, los servicios de seguridad se han acostumbrado a operar con impunidad dentro de las fronteras de Rusia, siendo acusados en reiteradas ocasiones de asesinar a los opositores políticos de Putin, conspirar para engañar a las normas de dopaje para ganar medallas olímpicas y proteger a los ciber delincuentes que actúan persiguiendo los intereses del Kremlin (Committee On Foreign Relations of The USA, 2018, p.18). De esta forma, se abrió un periodo de represión interna protagonizado por el control de los sectores más importantes de las economías locales, corrupción, luchar contra cualquier regionalismo que ponga en peligro la unidad nacional y territorial, llevar a cabo ofensivas de propaganda a través de todo un entramado de medios de comunicación y redes sociales, y desplegando una serie de estrategias con el fin de debilitar a los gobiernos que se resisten a las órdenes de Moscú.

2.2 Medios de manipulación

La red mediática rusa cuenta con mecanismos de propaganda muy diferentes entre sí, pero que se complementan los unos a los otros. Este trabajo ha señalado los más importantes y los que son más determinantes a la hora de comprender el caso de estudio, objeto del apartado siguiente. La visibilidad de estos medios de comunicación trata de dar una falsa imagen de trasparencia. Todo el mundo sabe de la existencia de las centrales de inteligencia rusa, sin embargo, ¿cómo funcionan? Asimismo, cualquiera podría conocer el origen ruso de los distintos medios de comunicación que serán objeto de estudio en este apartado, pero ¿qué hay detrás de una aparentemente inocente noticia?

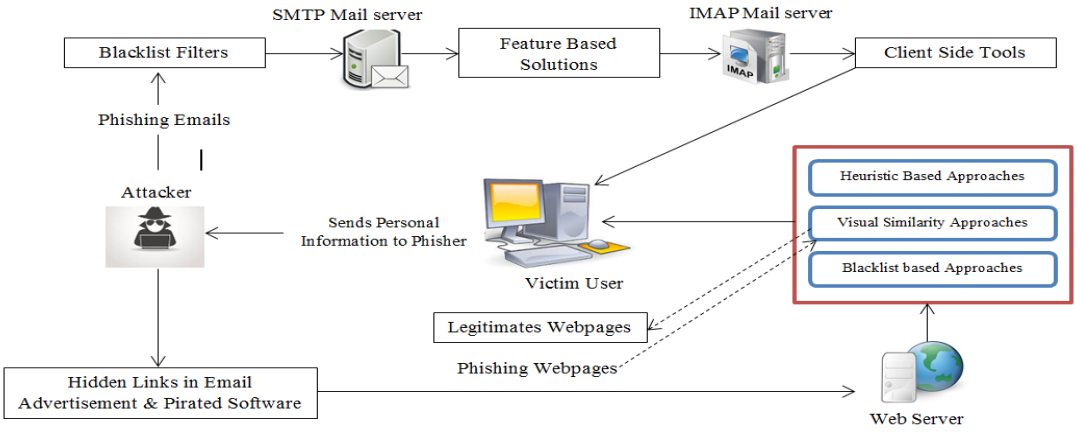
En efecto, el gobierno ruso cuenta con diversas centrales de inteligencia. Es imposible conocer todos los mecanismos que Rusia emplea para desarrollar sus ataques cibernéticos y sus peligrosas campañas propagandísticas. No obstante, como punto de partida, pueden ser señaladas dos de ellas, cuya eficacia ha sido demostrada en reiteradas ocasiones, especialmente tras los efectos de sus operaciones en las elecciones presidenciales americanas del año 2016, objeto de estudio del capítulo siguiente. Éstas centrales son conocidas como Main Intelligence Directorate (cuya abreviatura es GRU) y Federal Security Service (conocido con las siglas de FSB). Estos organismos desarrollan una serie de estrategias basadas en contrarrestar el poder de todo adversario,

sin necesidad siquiera de salir de Rusia (Singer, 2018, p.107).

Empleando la jerga relativa al campo de la ciberseguridad, dichas agencias utilizan las llamadas Amenazas Persistentes Avanzadas, también conocida por sus siglas en inglés APT (*Advanced Persistent Threat*). Esta técnica se caracteriza por tener objetivos muy concretos, en inglés *target*. Mediante una serie de discretas técnicas informáticas desarrolladas por *hackers*, adquieren suficiente información sobre el objetivo fijado como para controlar el sistema informático vinculado con el mismo. Para ello, utilizan técnicas de todo tipo, desde operaciones simples hasta otras más complejas, empleando todo tipo de programas informáticos, controlados por ingenieros especializados. A modo de avance, en los años previos a las elecciones americanas de 2016, dos grupos de hackers comenzaron a competir entre ellos. Lideraron las llamadas APT28 y la APT29, cuyos nombres claves fueron *Fancy Bear* y *Cozy Bear* respectivamente. El grupo de hackers que lideraba la batalla era aquel que lograba recoger la mayor cantidad posible de información que comprometiera al personaje público que supusiera una amenaza contra los intereses de Rusia, ya fuera un político, un periodista, un militar o académicos interesados en Rusia. En otras palabras, cualquier persona que se opusiera a los intereses de Putin (Watts, 2018, p.140).

Podría parecer que Rusia emplea una sofisticada red de dispositivos informáticos a la hora de desarrollar un nuevo ataque cibernético e infiltrarse en distintos sistemas. No obstante, no tiene por qué ser así. En la mayoría de los casos, el dispositivo informático ruso emplea las técnicas más básicas para tener acceso a las credenciales de los ciudadanos a la hora de iniciar sesión en sus respectivas cuentas de correo electrónico o redes sociales. Esta estrategia, llamada *Spearphising,* ha sido durante todos estos años el mecanismo más eficaz a la hora de acceder a las cuentas de usuarios de todo el mundo. Este anglicismo viene a significar el proceso por el cual los *hackers* tratan de robar las credenciales a los usuarios mediante sucesivos *spams*, o en otras palabras URLs que una vez seleccionados redirigen al usuario a un determinado servidor que descarga los popularmente conocidos virus. A partir de aquí, el ordenador infectado es una puerta abierta para el acceso a toda la información del usuario (Gupta, Arachchilage y Psannis, 2018, p.249). El motivo del brillante funcionamiento de esta técnica es que es muy sencillo convencer a un ser humano de que haga *click* en un determinado *link*. Es tan fácil como alarmarle de la importancia de cambiar su contraseña, alegando que alguien está teniendo acceso a sus cuentas. La siguiente imagen explica este proceso con mayor

claridad[2]:



Fuente: Gupta, B. B., Arachchilage, N. A., & Psannis, K. E. (2018).

Para comprender la manera de operar de la infraestructura rusa de medios de comunicación, es necesario hacer referencia al anglicismo *troll*, a día de hoy un término ampliamente utilizado en cualquier debate de ciberseguridad. Los *trolls* son usuarios "maliciosos" que intentan difundir una opinión o distorsionar las percepciones de la sociedad, acerca de un asunto determinado. La identificación de *trolls* en las redes sociales es una tarea de interés para muchas aplicaciones de *big data*, ya que los datos no pueden analizarse de manera efectiva sin, en primer lugar, localizar a estos usuarios ficticios entre la multitud. Pueden estar presente en cualquier red social, ya sea Twitter, Facebook o Instagram. A pesar de que cada vez existen varias técnicas para la detección de los mismos, la realidad es que numerosos usuarios que comenzaron abriéndose una cuenta personal acaban convertidos, voluntaria o involuntariamente, en *trolls* difusores de mensajes que pueden tener fines muy peligrosos (*IEEE International Conference on Big Data, 2016)*. Actualmente, existen numerosos testimonios de usuarios que han recibido notificaciones de Facebook, afirmando que su perfil hacía tiempo que no era actualizado. Es bastante frecuente que una persona se abra una determinada cuenta en una red social u otra, pero que no sea muy activa en redes sociales. Incluso es posible que llegue un punto en el que se olvide de la existencia de esa cuenta, que a pesar de haber llegado a un número considerable de contactos, queda inutilizada. Este es el escenario perfecto para un *hacker*, deseoso de convertir dicha cuenta en un *troll*. Es tan fácil como conseguir acceso atacando el sistema computacional empleado por el

[2] Lifecycle of phishing attacks based on phishing emails and phishing websites.

usuario. Una vez que se ha dado este paso, el *hacker* tiene libertad absoluta para compartir información acorde a sus fines, entre una gran cantidad de usuarios receptores que, por si fuera poco, pensarán que los mensajes están siendo emitidos por una persona real (Perry, 2018).

No obstante, esta no es más que la definición general de *troll*. Rusia emplea distintos tipos que conforman una sofisticada red capaz de producir resultados espectaculares. Además, el contenido que generan dichos *trolls*, puede pertenecer a varias categorías, aunque, generalmente, siempre buscan servir a los siguientes fines: puede consistir en una contradicción aparentemente sin sentido o contraria al conocimiento común, así como una manera de dirigirse de forma peyorativa a una persona concreta o a un determinado colectivo, con el fin de generar un aluvión de respuestas contra tales contenidos generados por el propio *troll*. Estos mensajes se transmiten por todo el mundo a miles de ordenadores, consiguiendo llamar la atención de millones de usuarios, suscitando, cuando menos, controversias importantes entre los distintos sectores de la sociedad (Indiana University, 2018). Entre los tipos de *troll* que destacan a la hora de desarrollar esta estrategia, se encuentran los llamados *hecklers* y los *honeypots*.

Los *hecklers* son los responsables de liderar la estrategia de la propaganda, haciendo que aumente la audiencia destinataria de los mensajes que emite la infraestructura de *trolls*. Para ello, difunden mensajes peyorativos sobre determinadas personas o colectivos, así como noticias alarmantes que, evidentemente, ni siquiera han de cumplir con requisitos de veracidad y coherencia. Para ello, la estrategia comienza "reclutando" a diversos perfiles de internet, simpatizando con usuarios en medios como *chats* donde se discuten temas online. Asimismo, este tipo de *troll* es el responsable de localizar a los usuarios que opinan de una forma distinta a la deseada, para bombardearlos con mensajes disruptivos y restarle repercusión a los mensajes que tales usuarios emitan y no sean del interés de los *trolls*, o más bien, de la persona que esté detrás de ellos (Watts, 2018, p.82).

Cuando los *hecklers* no logran frenar la oleada de opiniones contradictorias a sus intereses, utilizan como recurso a los *honeypots*. Singer define este tipo de instrumento como un "cebo" por al que un determinado usuario no se puede resistir, generalmente una cuenta falsa en una red social que simula pertenecer a una mujer atractiva (Singer, 2018, p.115). El objetivo de los *honeypots* es obtener cierta información comprometida, susceptible de ser empleada como mecanismo de extorsión para alcanzar los fines

deseados. El proceso comienza, en este caso, con un perfil de una determinada cuenta de una red social en el que una mujer atractiva envía mensajes del siguiente tipo: "podrías seguirme/agregarme? Tengo que decirte algo importante". A título de ejemplo, en Twitter, la mayoría de honeypots son cuentas correspondientes a este tipo de perfil expuesto, pero también es frecuente encontrar perfiles que simulan ser un afiliado a un partido político u otro. Cuando un usuario entabla una relación con un *honeypot*, estos *trolls* proceden a enviarle un mensaje con un link que, en caso de que el usuario acceda a él, le da al *troll* la capacidad para acceder al ordenador del usuario y poder obtener la información que desee. Asimismo, esta vía también es empleada para distribuir la propaganda que le interese a la persona que esté detrás de un trol (Watts, 2018, p.83).

El objetivo de los *trolls* no es otro que reclutar personas afines a una determinada causa, en el caso de Rusia, simpatizantes con los intereses del Kremlin. Esta finalidad recuerda exactamente a los objetivos de la época de la guerra fría en la que EEUU y la URSS se disputaban el control del mundo mediante el establecimiento de zonas de influencia. No obstante, esta vez se trata de medios no militares, mucho menos costosos que un ejército, que suponen menos esfuerzo y menos riesgos, pues basta con un simple *click* para que un hacker acceda a un determinado sistema informático que prive al usuario de toda su privacidad.

No obstante, no todo iban a ser ataques cibernéticos ocultos realizados por *hackers*. El Kremlin destina un amplio presupuesto a los medios de comunicación cuya repercusión es de interés para la consecución de los objetivos del gobierno, tanto dentro como fuera de las fronteras rusas. Para entender el curso de las elecciones presidenciales de Estados Unidos del 2016, objeto de estudio del siguiente apartado, es necesario hacer mención previamente a dos de los principales medios de manipulación financiados por el gobierno ruso: la plataforma online emisora de noticias multimedia, Sputnik, editada por la agencia rusa de Rossiya Segodnya, y Russia Today (RT), ambas financiadas por el gobierno ruso (Ioffe, 2010). Estos medios de comunicación son empleados para desarrollar el llamado *soft power*[3], correspondiente a la habilidad de los Estados de alcanzar sus objetivos mediante la persuasión necesaria para influenciar el comportamiento de otros actores políticos, empleando medios ideológicos como puede ser, en este caso, una cadena de televisión o una página web. Se diferencia del *hard power* en que este último supone el empleo de la fuerza o recursos militares. Sin

[3] "Poder blando" en su traducción literal al castellano.

embargo, en la era de las telecomunicaciones, no puede negarse la importancia tanto de uno como de otro (Yang y Yuan, 2018, p.54).

La finalidad de RT y Sputnik es mejorar la imagen de Rusia, crear una opinión favorable para que la población simpatice con los intereses del Kremlin, quebrando la credibilidad de las democracias liberales de Occidente. Desde la creación de RT en el año 2005, y de Sputnik en el 2014, el Kremlin confía plenamente en la efectividad de estas plataformas. Casi 15 años después, su finalidad es clara. Estos medios son un auténtico propulsor de las llamadas *fake news*. El origen de este término se remonta a un estudio realizado por la Universidad de Oxford que muestra cómo las teorías conspiratorias y las historias que no son ciertas tienen, hoy en día, mayor repercusión que las noticias verídicas. En efecto, la combinación de la publicación de *fake news* en los medios de comunicación se ve propulsada por las redes sociales, generando resultados espectaculares. El estudio citado analizó 22 millones de *tweets,* concluyendo que los que eran falsos eran los que más habían sido compartidos por los usuarios. De esta forma, el término *fake news*, originariamente conocido como *junk news,* se ha consolidado en nuestro lenguaje para hablar de aquél contenido que es verificablemente falso. No obstante, este tipo de noticias tienen tanta repercusión, que para cuando se demuestra su falsedad ya han causado los efectos deseados (Singer, 2018, pp.130-131)[4].

El significado de este término concuerda con otro de connotación muy parecida: la desinformación. En el año 1949 el propio *Diccionario de la Lengua Rusa* incluyó la palabra *Dezinformatsia* como "acción de inducir a error mediante el uso de informaciones falsas", definición más que útil para comenzar a hablar del significado que tiene este término en la actualidad. Efectivamente, hoy en día su uso supone un juicio ético-demostrativo negativo, pues generalmente se refiere a ideas tergiversadas o manipuladas por aquellos que tienen acceso a los datos verdaderos, con el fin de crear o fomentar ciertas ideologías, comportamientos, actitudes y marcos referenciales (Romero, 2012). A pesar de que este concepto tiene casi tantos significados como autores que lo han estudiado, parece que un elemento común en las distintas definiciones es la falta de adecuación de lo que se comunica con la realidad de una determinada situación. En el campo de las Relaciones Internacionales, la desinformación es considerada una técnica de manipulación de las masas y la opinión pública (Rodríguez, 2013, p. 320).

[4] Ver anexo 1

Retomando la explicación de las operaciones desarrolladas por RT y Sputnik, ambas cadenas son las encargadas de difundir y amplificar toda noticia desfavorable a Occidente que revele su decadencia, dirigiéndose especialmente a dos tipos de espectadores: los ciudadanos rusos y los miembros de grupos radicales, ya sean de derecha o de izquierda, dentro de los países donde emiten las distintas noticias, logrando así el mayor impacto posible en las redes sociales (Singer, 2018, p.108). No obstante, la polémica está servida. YouTube, Twitter y Google han mostrado importantes reservas con estos medios. Concretamente, la propia portavoz de Google, Andrea Faville, calificó el contenido de las noticias divulgadas por dichos medios como "de baja calidad, falso y deliberadamente engañoso" (Dave y Stubbs, 2017). Sin embargo, sus severas palabras no han logrado evitar la repercusión de estas cadenas de comunicación, considerándose hoy en día como un elemento más de la política exterior de Putin, logrando en muchas ocasiones que el resto de fuentes de información parezcan menos fiables y haciendo que parezca que son el resto de Estados del mundo los que mienten a su población. Tal es la confianza del Kremlin en la efectividad de estas plataformas, que el presupuesto que recibe RT ha evolucionado, pasando de recibir 30 millones de dólares al año, en su origen, en el año 2005, a 400 millones de dólares al año en el año 2015. Asimismo, RT publica contenido en 6 idiomas: ruso, alemán, español, inglés, árabe y francés. Por su parte, Sputnik está presente en 130 ciudades y 34 países (Singer, 2018, pp.108-109).

Un caso de estudio que puede servir como ejemplo de la manera de proceder de RT y Sputnik fue la divulgación de noticias que realizaron durante la celebración del pasado referéndum ilegal de Cataluña. No parece una mera casualidad que en los días previos y siguientes a tal acontecimiento, entre las noticias más compartidas en Facebook y Twitter sobre la crisis catalana se encontraran las de RT, que tenía perfectamente estudiado el tipo de mensajes que debía emitir para causar la repercusión deseada. Noticias como "*El nuevo mapa de Europa: ¿Quiénes apoyan la independencia de Cataluña?"*, mensaje que traía adjuntado un gráfico que decía plasmar los Estados que reconocerían al "nuevo Estado catalán", produjeron más de 5.000 interacciones en Facebook en tan solo unas horas (Alandete, 2018)[5].

Gran parte del atractivo de RT y de Sputnik reside en la gran magnitud de contenido sensacionalista que publican. Según un estudio realizado en 2016 por RAND

[5] Ver anexo 2

Corporation, RT y Sputnik son, en realidad, una combinación de información y entretenimiento que una fuente periodística comprobada, aunque sus formatos traten de dar la apariencia de programas informativos adecuados. Esta fuente afirma que RT llegó incluso a realizar entrevistas falsas con actores a los que les pagó para que fingieran que eran víctimas de la agresión del gobierno ucraniano (Paul y Matthews, 2016).

Debido a la existencia de todos estos mecanismos, es inevitable que aparezcan en la esfera política términos como la propaganda computacional, más que conocido y empleado por el Kremlin. Esta estrategia consiste en combinar la desinformación con la manipulación digital para distribuir información engañosa a través de las redes sociales. La propaganda computacional implica imitar a personas reales para manipular la opinión pública a través de una amplia gama de plataformas y redes de dispositivos, labor realizada por los *trolls*, tal y como se ha explicado anteriormente. Se trata de una serie de tareas repetitivas y automatizadas, tanto relativas a la recopilación de información, como al reclutamiento de opiniones. El uso de Rusia de los *trolls* tiene fundamentalmente fines políticos, pues son herramientas efectivas para fortalecer la propaganda pro rusa y las campañas de odio hacia todo adversario, logrando en muchas ocasiones generar la ilusión de un consenso a gran escala para influir en el curso de las campañas electorales de los distintos Estados. Para ello, algunos de los elementos claves empleados son las explicadas *fake news* y los datos privados que pongan en entredicho las carreras profesionales de sus víctimas, así como su credibilidad (Woolley y Howard, 2017).

Tal es la estrategia que conlleva la propaganda computacional, que los *trolls* están diseñados para, en ocasiones, no solo emitir ciertos mensajes, sino para contestarse entre ellos y generar así el debate deseado. Por ahora, la red social en la que son más frecuentes es Twitter, pero esto no quita que estén presentes en cualquier plataforma digital, manipulando la opinión pública y apareciendo especialmente en momentos de incertidumbre política en los que es fácil polarizar las opiniones de los usuarios. Lo que está claro es la carencia de información de la mayoría de usuarios al respecto, muchos de ellos incluso menores de edad. Pocas son las personas que no son vulnerables a estos ciberataques. Se trata pues, de toda una herramienta de control social y un propulsor para la desinformación (Howard y Kollanyi, 2016).

Antes de analizar el significado de este último término, cabe realizar una aclaración: a pesar de que es frecuente confundir el término *troll* con *bot*, no son lo mismo. Los

bots son programas informatizados que son programados para realizar tareas repetitivas y que pueden generar *trolls*. Pero mientras el *troll* es un usuario que corresponde a una persona, ficticia o no, el *bot* es un programa informático que no solo genera *trolls*, sino que puede realizar otras muchas funciones, como rastrear información (Gianvecchio, Wang y Jajodia, 2010).

La aplicación práctica de los *trolls* y el uso de ello será tratada con detalle en el siguiente apartado. Sin embargo, no está de más ejemplificar cómo Rusia se sirvió del uso de *bots* generadores de miles de *trolls* cuando, en el año 2012, decidió que sus dos principales cadenas de comunicación, RT y Sputnik, aumentaran su presencia, pasando a tratar temas internacionales en vez de meramente asuntos internos. En realidad, en vez de temas internacionales estaría mejor dicho temas occidentales, y, para más detalle, toda información que pudiera mostrar indicios de la decadencia de las democracias europeas o norteamericanas. Rusia desarrolló todo un entramado de *trolls*, que tenían que llegar al día a un número mínimo de publicaciones, como si de cualquier trabajo se tratase. Invirtió en traductores que publicaran las noticias en inglés y promovió que Russia Today fuera más bien conocido como RT, pues así la primera imagen que cualquiera obtuviera de una publicación procedente de este medio, no mostraría tan fácilmente que se trataba de una redacción rusa (Watts, 2018, p.92).

Según una investigación realizada por *The New York Times*, en el año 2015 cientos de jóvenes rusos trabajaban en una auténtica empresa de *trolls*, esta vez situada en San Petersburgo, pues como después se citará, en muchos caso esta infraestructura es establecida en el propio país que va a ser destinatario del ciberataque en cuestión. Bajo la denominación de Agencia de Investigación de Internet (IRA por sus siglas en inglés), esta empresa empleó a una gran magnitud de trabajadores, cuya cantidad exacta se desconoce, que trabajaban turnos de 12 horas en departamentos enfocados a diferentes plataformas de medios de comunicación y redes sociales (Chen, 2015). Una entrevista de la NBC de un ex trabajador de IRA, Vitaly Bespalov, reveló que los trabajadores estaban altamente equipados para amplificar el trabajo realizado por el resto de medios de comunicación. Esta organización centró su actividad principalmente en escribir publicaciones para promover la intervención de Rusia en Ucrania. Mientras que algunos *trolls* escribían y publicaban dichas noticias, otros se dedicaban a opinar en las redes sociales sobre ellas, utilizando falsas identidades ucranianas. Estaba todo planeado. Antes de que los redactores comenzaran a publicar tales noticias, recibían una lista de

opiniones que debían difundir y de temas que debían tratar. Durante cada jornada laboral, cada trabajador debía publicar al menos 5 noticias de contenido político, pero a su vez unas 10 que tuvieran otro tipo de contenidos, con el fin de aumentar la credibilidad de estos falsos usuarios. Asimismo, cada *troll* debía publicar entre 150 y 200 comentarios sobre las noticias publicadas por el resto de compañeros. El salario medio era de unos 41.000 rublos al mes (casi 800 dólares americanos), un salario atractivo para muchos jóvenes (Popken y Cobiella, 2017). Las investigaciones apuntan a que IRA fue financiada por un socio cercano de Putin, Evgeny Prigozhin, un rico propietario de una cadena de restaurantes, también conocido como el "Chef del Kremlin", incriminaciones que proceden de la existencia de una red de de contratos gubernamentales lucrativos que poseía en su poder. De hecho, en 2016 fue denunciado por el gobierno de Obama por haber contribuido al conflicto de Ucrania (Chen, 2015).

Tales han sido los esfuerzos de Rusia y los medios invertidos en la armada de *trolls*, que actualmente, los suscriptores al canal de RT en YouTube, han alcanzado a los que posee la CNN. Sin embargo, es curioso que las noticias que RT distribuye por redes sociales como Twitter, a menudo no eran publicadas en ninguna televisión rusa, por no hablar de que muchas de ellas no aparecían en ningún medio de comunicación de los Estados occidentales. Sputnik no fue menos, y desde 2012 ha multiplicado las noticias sensacionalistas, cualquiera que pudiera perturbar al espectador con teorías conspiratorias y promover la idea de que Occidente está inmerso en el más puro estado de corrupción. Asimismo, una de las brillantes estrategias desarrolladas por los *trolls*, es hacer a numerosos usuarios cómplices de Rusia, sin que ni siquiera ellos lo sepan. ¿Cómo? Cada vez que una persona escriba un simple *tweet* cuyo contenido favorece a Rusia, el sistema de *bots* lo localiza y hace que los *trolls* rusos compartan dicho tweet para que tenga la repercusión deseada. De esta forma, simples usuarios, muchas veces con escasos seguidores, sienten que publicar este tipo de opiniones aumenta su popularidad, por lo que comienzan a difundir más contenido con estos mensajes (Watts, 2018, p.21).

Para concluir este apartado, es interesante mencionar las teorías existentes sobre una posible estrecha relación entre Rusia y WikiLeaks. Por si el entramado de medios de manipulación no fuera suficiente, es inevitable sumarle a este estudio el cambiante comportamiento de WikiLeaks desde que su fundador, Julian Assange, comenzó en el año 2006 una campaña para promover la transparencia y la libertad de información,

criticando a los Estados que censuraban información clasificada con el fin de controlar a una población engañada, tal y como expresó al publicar su propio manifiesto "Conspiracy as Governance". En un principio, Assange no era más que un *hacker*, como la mayoría de informáticos activistas que abogan por la transparencia. Assange pretendía luchar tanto contra tales gobiernos, a los que denominó conspiradores, como contra los organismos y personas que trabajaran para ellos, concretando como destinatarios de sus próximo ataques: China, Rusia y Eurasia Central (Khatchadourian, 2010). Si bien es cierto que en los tres primeros años de WikiLeaks, las filtraciones de información afectaron principalmente a China, Kenya, miembros de la secta de la cienciología, y de forma creciente a Estados Unidos, en el año 2010 Assange aclaró que Rusia no se libraría de las filtraciones de información que WikiLeaks estaba llevando a cabo. En una entrevista en el periódico pro ruso *Izvestia* dijo, expresamente, que WikiLeaks tenía mucho material de Rusia que pronto saldría a la luz y que haría que "*los rusos descubran información muy interesante sobre su propio país*" (Weir, 2010). El mundo entero esperaba ansioso a que tales afirmaciones se materializaran con filtraciones de información que podrían haber cambiado el curso de las relaciones internacionales. Sin embargo, los secretos de Rusia nunca salieron a la luz de la mano de WikiLeaks. Se desconoce el por qué, y no hay pruebas de que Rusia sea la responsable, pero la realidad es la siguiente: mientras que EEUU ha sido fuertemente golpeado por las filtraciones de WikiLeaks, Rusia ha salido, en comparación, intacto (Watts, 2018, p.106).

2.3 Caso de estudio: Las Elecciones Americanas de 2016

El presente caso de estudio ha sido analizado con el apoyo de dos documentos elaborados por el propio gobierno estadounidense: una denuncia planteada ante la Corte del Distrito de Columbia, y un informe realizado por el Comité de Asuntos Exteriores del Senado.

La denuncia fue interpuesta por el fiscal Robert Swan Mueller III. En este documento, EEUU forma parte de la acusación, denunciando desde la exposición de motivos de dicho documento, injerencias extranjeras en asuntos de política interna relativos, fundamentalmente, al curso de las elecciones presidenciales de 2016. La defensa está constituida por la *Internet Research Agency*, que es una organización rusa acusada de interferir en las elecciones americanas. La acusación no se limita a nombrar

a una organización, sino que acusa con nombres propios a miembros de la misma. De acuerdo con la denuncia, las operaciones de injerencia en dichos procesos electorales comenzaron en el año 2014, culminando en las elecciones presidenciales de 2016. La agencia es acusada de haber recibido fondos provenientes de una persona de nacionalidad rusa llamada Yevgeniy Viktorovich Prigozhin, así como de las empresas que dicha persona posee, incluidas: Concord Management And Consulting y Concord Catering, ambas registradas como entidades corporativas en Rusia desde 2013 (Mueller, 2018, p.5)[6]. Como prueba, la acusación alega que cuenta con numerosos contratos firmados entre ellas, principalmente de financiación. Otro nombre propio que forma parte de la defensa es el de Mikhail Ivanovich Bystrov, que se unió a Concord en febrero de 2014, convirtiéndose posteriormente en su presidente ejecutivo. El gobierno estadounidense tiene pruebas de las reuniones que las personas acusadas mantuvieron, así como del contenido de las mismas, involucrándolas de forma directa en este caso (Mueller, 2018, p.8). Estos son solo algunas de las personas denunciadas en dicho documento, pues existen pruebas de la participación de al menos otros 10 directivos, denunciados con su nombre propio y por operaciones concretas relacionadas con la causa. Todos ellos se unieron a CONCORD en el año 2014.

Concretamente, las acusaciones de EEUU afirman que CONCORD creó numerosas cuentas falsas, revestidas de apariencia americana, destinadas a movilizar a la audiencia en las redes sociales, con el propósito de interferir en el resultado de las elecciones del 2016 (Mueller, 2018, p.3). En efecto, este documento plasma que los acusados realizaron diversos gastos con el fin de comprar anuncios políticos en las redes sociales a nombre de personas y entidades de los Estados Unidos. Asimismo, la defensa denuncia que Concord promovió manifestaciones políticas dentro de los Estados Unidos. La manera de no levantar sospechas era tener como base el territorio estadounidense. Todas estas operaciones se desarrollaron desde dentro. Además, todo usuario emisor de mensajes insurgentes se hacía pasar por un norteamericano, sin revelar sus identidades rusas y su afiliación a las distintas unidades empresariales, bajo el control de CONCORD. Asimismo, según la defensa, las personas acusadas pagaron a personas reales de los Estados Unidos para que hicieran buena o mala propaganda de los candidatos. Las operaciones se desplegaron por YouTube, Facebook, Instagram y Twitter. La exposición de motivos de este documento prosigue explicando lo siguiente:

[6] A partir de ahora se empleará el término CONCORD para referirse a ambas.

En el año 2014, los acusados comenzaron a rastrear y analizar los medios de comunicación y las cuentas de redes sociales que trataban asuntos políticos y sociales en EEUU. Dicho análisis se centró en la repercusión que tales medios tenían, la frecuencia con la que incorporaban nuevos contenidos y la participación y reacciones de la audiencia al respecto, midiendo el número de comentarios o *likes* que obtenían de promedio las publicaciones de tales cuentas. Una vez estudiado este punto, comenzaron los viajes a EEUU para estudiar el terreno de primera mano. Los demandados planificaron cuidadosamente cuáles serían los motivos que alegarían con el fin de obtener acceso al país, normalmente solicitando los visados correspondientes a cualquier viaje turístico, en vez de reconocer que se trataba de un viaje de negocios, con el fin de evitar sospechas. Una vez dentro del territorio, procedieron a la compra del equipo informático necesario para que los ordenadores utilizados para desarrollar las diversas operaciones de manipulación no revelaran el origen ruso de las mismas. De esa forma, cuando los expertos estadounidenses rastreaban la señal, podían comprobar que esta no excedía las fronteras de Estados Unidos.

La acusación afirma que las empresas involucradas emplearon cientos de individuos para realizar las operaciones *online* mencionadas. Consistía en una infraestructura perfectamente organizada y jerarquizada, con un departamento de análisis de datos, un departamento de optimización de motores de búsqueda, de tecnología de la información, mantenimiento y un departamento de finanzas encargado de asignar los fondos necesarios para el desarrollo de los ciberataques. De hecho, CONCORD recibió más de 73 millones de rublos, distribuidos en 14 bancos estadounidenses. La justificación alegada para entrar en el país era apoyar el desarrollo tecnológico de CONCORD, cuyos fines se desconocían entonces. No obstante, para evitar sospechas por la acumulación de tal capital en una única empresa, se crearon numerosas filiales, entre las que se encuentran Glavnaya Liniya LLC, Merkuriy LLC, Obshchepit LLC, Potentsial LLC, RSP LLC, ASP LLC, MTTs LLC, Kompleksservis LLC, SPb Kulinariya LLC, Almira LLC, Pishchevik LLC, Galant LLC, Rayteks LLC, y Standart LLC.

Los empleados de las distintas filiales se dividieron el trabajo. Mientras que algunos trabajaban de día, otros emitían *posts* de noche, adaptándose al perfil del receptor en función de la franja horaria que se tratara. Dichas publicaciones trataban todo tipo de temas sensacionalistas, desde económicos hasta sociales, sobre todo relacionados con la inmigración y la política exterior de EEUU. Las instrucciones que recibieron eran

claras: debían crear un espíritu en las redes sociales de apoyo a grupos radicales, usuarios insatisfechos con su situación económica o política y determinados movimientos sociales. En Facebook e Instagram, tal movimiento se materializó mediante la creación de diversos grupos, en los que se discutían permanentemente estos temas, retroalimentando el descontento de los lectores. Cualquier colectivo insatisfecho tenía cabida en esta estrategia. Algunos ejemplos de las páginas de Facebook que se crearon fueron: *Secured Borders*, para tratar asuntos relacionados con la inmigración, *Blacktivist*, como respaldo del movimiento *Black Lives Matter*; o *United Muslims of America* y *Army of Jesus* con carácter religioso. Asimismo, en relación a la población de determinadas regiones de EEUU, se crearon páginas como *South United* y *Heart of Texas*. Para 2016, el tamaño de estos grupos, controlados por CONCORD, había crecido a cientos de miles de seguidores en línea. Asimismo, fueron creadas numerosas cuentas de Twitter diseñadas para que pareciera que eran controladas por personas o grupos estadounidenses. Un ejemplo es la cuenta "Tennessee GOP", que usó como usuario @TEN_GOP, y afirmó, falsamente, estar controlada por un partido político estadounidense. Dicha cuenta llegó a atraer a más de 100.000 seguidores en línea. Para medir el impacto de sus operaciones de redes sociales en línea, los demandados rastrearon el rendimiento del contenido que publicaron en dichas redes sociales, fijándose especialmente en el aumento de los seguidores de dichas cuentas, que eran estadounidenses. Como prueba de ello, Mueller aportó en la denuncia citada algunos de los informes de datos métricos que la organización rusa desarrolló para el estudio de la influencia que estaba teniendo en los medios, así como las instrucciones que los empleados recibieron para mejorar la calidad de sus publicaciones, que versaban sobre temas como proporciones de texto, gráficos y videos útiles para su cometido, el número de cuentas a operar y el rol de cada cuenta.

No obstante, una de las acusaciones realizadas por el gobierno de EEUU es la usurpación de identidad de verdaderos ciudadanos estadounidenses, sin su conocimiento ni mucho menos consentimiento. Esto les sirvió para abrir cuentas de PayPal, realizar pagos por Internet y por supuesto, publicar cierta información en su nombre, utilizando sus cuentas personales, accediendo a sus contraseñas y cuentas de email.

Para la acusación, el objetivo de Rusia estaba claro: el gobierno de Putin tenía un plan estratégico para crear la controversia necesaria en EEUU que alejara a diversos

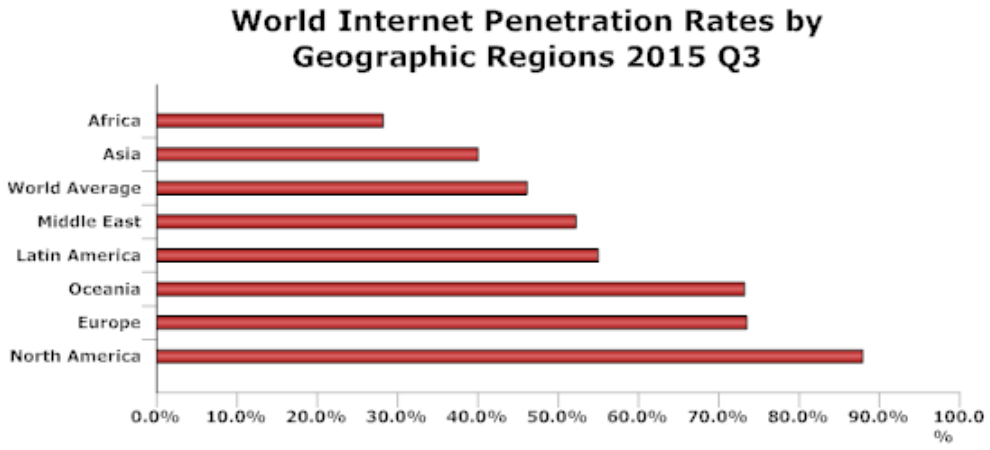
candidatos de las urnas. Posteriormente, dicho plan se concretaría en apoyar la candidatura de Trump y conseguir el fracaso de Clinton.

"In order to carry out their activities to interfere in U.S. political and electoral processes without detection of their Russian affiliation, Defendants conspired to obstruct the lawful functions of the United States government through fraud and deceit, including by making expenditures in connection with the 2016 U.S. presidential election without proper regulatory disclosure; failing to register as foreign agents carrying out political activities within the United States; and obtaining visas through false and fraudulent statements" (Mueller, 2018, p.4).

Sin embargo, este objetivo no parecía tan evidente cuando tales operaciones comenzaron en el año 2014. En un principio, parecía que Rusia se conformaba con impregnar de desconfianza el sistema político americano en su totalidad. Sin embargo, ya en el año 2014 EEUU tenía motivos para alarmarse tras los ataques cibernéticos desarrollados por el grupo pro ruso CyberBerkut, formado por una serie de *hackers* que seguían órdenes directamente del Kremlin. Los ataques se dirigieron concretamente contra la Comisión Central de las Elecciones Ucranianas, manipulando el resultado electoral con el fin de que ganara las elecciones el candidato que más le convenía a Rusia: Dmytro Yarosh. El gobierno ucraniano descubrió tal operación antes de que los resultados salieran a la luz. No obstante, Rusia no aceptó su derrota, y como represalia pocas fueron las empresas e instituciones del gobierno ucraniano que se libraron de sufrir más ataques cibernéticos, por no mencionar como cúspide de dichos ataques el conocido como *Black Energy*, que dejó sin electricidad a toda la región ucraniana de Ivano-Frankivsk durante el mes de diciembre del año 2015 (Watts, 2018, p.139). Rusia había cogido práctica y estaba preparada para centrarse en su siguiente objetivo: las elecciones americanas.

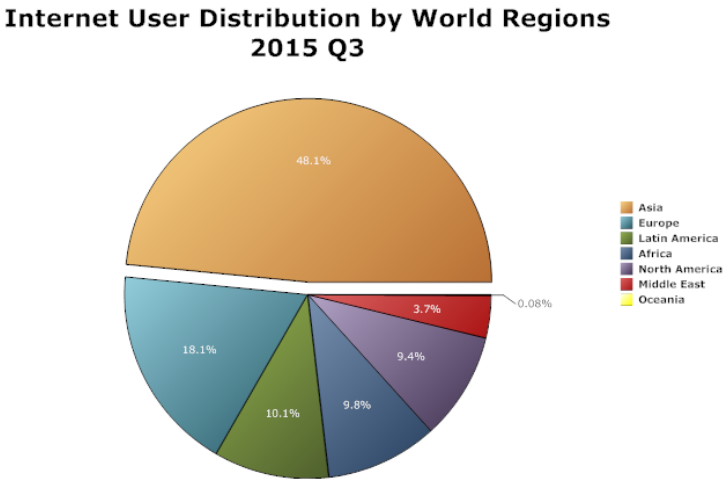
Tras los viajes realizados por los agentes rusos miembros de la organización CONCORD y la infraestructura situada dentro de las fronteras estadounidenses, los *hackers* rusos poseían suficiente información para atacar, a las puertas de la campaña electoral que precedería a las elecciones presidenciales del 2016. Los trabajadores de CONCORD habían robado información basada en datos personales de ciertos protagonistas de la campaña, lo suficientemente graves como para hundir su reputación y acabar con su carrera política. Los *hackers* rusos no tardaron en tener acceso a miles de cuentas de e-mail y bases de datos de instituciones americanas. Cualquier dato que

pudiera parecer creíble y fuera susceptible de causar confusión era más que bienvenido, fuera verídico o no. Autores como Clint Watts han definido este ataque cibernético como la mayor y más sofisticada red de hackers de la historia (Watts, 2018, p.140). Además de la infraestructura explicada anteriormente, existen pruebas de la participación de dos Agencias de Inteligencia Rusas: Main Intelligence Directorate (GRU) y Federal Security Service (FSB), empleando las técnicas de Amenaza Persistente Avanzada, explicadas en el capítulo anterior. No era de extrañar que el *Spearphising*[7] fuera un éxito en esta nueva misión.



Fuente: Gupta, B. B., Arachchilage, N. A., & Psannis, K. E. (2018).

De acuerdo con esta gráfica, Norteamérica es la región del mundo en la que internet tiene una mayor incidencia, incluso aunque no sea la región que más usuarios de internet albergue en el mundo, acorde a esta segunda gráfica:



Fuente: Gupta, B. B., Arachchilage, N. A., & Psannis, K. E. (2018).

[7] Ver anexo 3.

La estrategia conocida como *Kremlim Election Wave* comenzó a finales del año 2015, a raíz de las injerencias en el Comité Nacional Demócrata, organización que gobierna el partido democrático estadounidense, supervisando el apoyo a las campañas y actividades políticas de los candidatos del partido a las elecciones. Asimismo, esta entidad es la responsable de la recaudación de fondos (Richardson, 2018). En septiembre de ese mismo año, el agente del FBI, Adrian Hawkins, informó mediante un mensaje de voz al responsable del soporte técnico del Comité, Yared Tamene, sobre las posibilidades de un ciberataque a la base de datos de la organización, bajo riesgo de que los hackers pudieran tener acceso a información confidencial. Las sospechas infundadas del agente provenían de sus años de estudio y rastreo de un grupo pro ruso sospechoso de estar desarrollando ciber espionaje que se hacían llamar "The Dukes". Las acusaciones del agente no fueron suficientes para evitar el ataque, y el Comité se vio desbordado por las constantes operaciones APT28 y APT29. Gracias a estas técnicas, los rusos tuvieron acceso al sistema informático del comité durante siete meses, lo que les permitió robar información confidencial y tener acceso a las cuentas de email de los candidatos a las elecciones. El Partido Republicano tampoco se libró de los ataques cibernéticos. No obstante, no tuvieron, ni mucho menos, la incidencia y el impacto que supusieron para el Partido Demócrata. Esta vez, los hackers se centraron especialmente en dos individuos, los senadores Lindsey Graham y John MacCain, tachados por Putin de adversarios de Rusia (Watts, 2018, pp.141-142).

En el año 2016, tuvo lugar un nuevo ataque que supuso un punto de inflexión en la campaña de Hillary Clinton. John Podesta, su director de campaña, recibió un email cuyo remitente era, aparentemente, Google, informándole de que alguien estaba intentando acceder a su cuenta de gmail, y que por lo tanto debía proceder a cambiar su contraseña inmediatamente accediendo a un *link*. Como el partido Demócrata ya había sido advertido de los posibles ataques cibernéticos rusos, Podesta procedió a consultar la veracidad del mensaje recibido con uno de los técnicos del partido: Charles Delavan, que le contestó a Podesta que podía confiar en dicho email. Y así es como los hackers rusos tuvieron acceso a su cuenta, concretamente a más de 6.000 emails. Sin embargo, la historia no termina aquí. Charles Delavan escribió un mensaje a John Podesta diciendo que el mensaje recibido por Google era "legítimo" *("This is a legitimate email")*. Pero atención: cuando el acceso de los rusos a los emails fue conocido, Delavan dijo que creía haber escrito ilegítimo. Una simple letra fue la que hizo que

Podesta cayera en la trampa (Uchill, 2016). ¿Error, casualidad o de nuevo una estrategia rusa?

En al capítulo anterior se mencionó que se ha cuestionado en numerosas ocasiones la relación entre WikiLeaks y el Kremlin. Esta hipótesis resurgió el año 2016, precisamente a causa del ataque cibernético que sufrieron los servidores de los ordenadores del partido Demócrata. ¿Qué ocurrió con todos los emails sustraídos de la bandeja de entrada de Hillary Clinton? El 16 de marzo, en plenas primarias, WikiLeaks filtró los emails a los que los *hackers* rusos habían tenido acceso, proporcionando en tal filtración un buscador por el que cualquiera podría localizar una palabra clave dentro de los miles de emails revelados. Más de 50.000 páginas de email de Hillary Clinton al descubierto[8]. Toda persona que no simpatizara con Clinton, ya fuera un adversario político o un simple votante, podría aprovechar la situación para buscar información que comprometiera la carrera política de la demócrata, por no hablar del juego que esta situación le daba a los periodistas. Por si fuera poco, los simpatizantes de Donald Trump clamaban en sus meetings políticos por la supresión de la candidatura de Clinton, debido a su irresponsabilidad al permitir que saliera a la luz información clasificada. ¿Filtró el gobierno ruso los emails a WikiLeaks, o nos encontramos de nuevo ante una mera coincidencia? O lo que es más grave, el 5 de julio de este mismo año, el director del FBI, James Comey, dio por finalizada la investigación y recomendó activamente que no se presentaran cargos. La investigación no fue, supuestamente, reabierta hasta finales de octubre de 2016 (Watts, 2018, p.151).

Las filtraciones de los emails fueron más allá, atacando en mayo de 2016 a la propia Convención Nacional Demócrata, filtrando una serie de emails en los que miembros del partido Demócrata solicitaban a la Convención la supresión de la campaña de Bernie Sanders, mostrando, por ejemplo, cómo personalidades, como Debbie Wasserman Shultz, demostraban en los emails un claro favoritismo hacia Clinton. La red de *trolls* rusa aprovechó esta información para que se divulgara una imagen de un Partido Demócrata corrupto que conspiraba contra Sanders.

Por si fuera poco, Rusia no se conformó con una investigación que finalizara sin presentar cargos contra sus agentes. En junio de ese mismo año, apareció en las redes

[8] Actualmente, sigue siendo posible acceder al contenido de dichos emails en el siguiente link: https://wikileaks.org/clinton-emails/.

una persona que se hacía identificar con el usuario Guccifer 2.0, reivindicando la filtración de emails a WikiLeaks. El análisis realizado por los servicios de inteligencia estadounidenses especializados en ciberseguridad concluyó que los ciberataques realizados a los servidores de los ordenadores de la Convención Nacional Demócrata y a Hillary Clinton habían sido provocados por la APT28 y APT29, y no por esta persona que se hacía llamar Guccifer 2.0. Además, el tal Guccifer afirmó ser rumano, pero ciertas señales técnicas revelaron que dicho dato no era cierto, pues no sólo cometía numerosos errores, que demostraron que el rumano no era, ni mucho menos, su lengua materna, sino que además, el email que estaba utilizando procedía de una Red Privada Virtual (RPV) de origen ruso (Watts, 2018, pp.146-148), mecanismo que consiste en la extensión de una red privada que abarca enlaces a través de redes compartidas o públicas como Internet, lo que le permite a su usuario enviar datos entre dos ordenadores a través de una red pública o compartida transfiriendo información de un enlace privado a otro. La utilidad reside en que para que la información pueda ser transportada mediante este mecanismo, es cifrada y encriptada, proveyéndola de total confidencialidad, convirtiéndola en indescifrable sin unas determinadas claves. La parte de la conexión en la que se encapsulan los datos privados se conoce como el túnel. La parte de la conexión en la que se cifran los datos privados se conoce como conexión de red privada virtual (Microsoft, 2009).

La conclusión inmediata fue que el Kremlin había intentado disuadir el curso de las investigaciones, con el fin de desviar la atención de sus operaciones y que no fuera culpado. Sin embargo, la gravedad del asunto aumentó cuando Guccifer 2.0 filtró más información confidencial del Comité Nacional Demócrata, concretamente un documento que analizaba los puntos débiles de los distintos miembros del partido, con el fin de probar que efectivamente él había sido el responsable de las filtraciones de los emails de Hillary Clinton. Si bien es cierto que la relación entre el gobierno ruso y Guccifer 2.0 había sido descubierta, parece que Rusia no era la única interesada en que se asignara la responsabilidad del ciberataque a tal sujeto. El 10 de agosto de ese mismo año, Roger Stone, asesor de Donald Trump, calificó a Guccifer 2.0 en su cuenta de Twitter como un héroe por haber puesto a disposición de la población información de tal importancia (Watts, 2018, p.148). Y por si aún quedaban dudas sobre la concordancia de intereses de WikiLeaks y el gobierno ruso, los acontecimientos de 2016 despejaron todo tipo de dudas. A pesar de la velocidad con la que Trump ganaba

simpatizantes, sus posibilidades de ganar las elecciones se pusieron en entredicho cuando el *Washington Post* publicó un video en el que se mostraba a Donald Trump emitiendo un mensaje machista, presumiendo del control que tenía sobre su mujer. La repercusión fue inmediata. En menos de una hora desde la publicación del video, WikiLeaks había respondido con la filtración de miles de emails provenientes del servidor de John Podesta.

Mientras tanto, los *trolls* se multiplicaron en todas las redes sociales. Los mensajes propagados tachaban a Hillary Clinton de persona conflictiva, proclive a llevar a los EEUU a una guerra contra Rusia. Sin embargo, el futuro resultado de las elecciones seguía siendo una incógnita para Rusia. Por ello, durante la etapa de primarias, el Kremlin consideró que lo más práctico era abogar por la victoria tanto del candidato demócrata como del candidato republicano que más conviniera a los intereses de Rusia. Los elegidos fueron Bernie Sanders y Donald Trump. Los *trolls* intensificaron su actividad y la propaganda a favor de estos dos candidatos, que sumada a sus propias campañas electorales, lograron que la opinión pública los tuviera cada vez más en cuenta (Watts, 2018, p.150).

Una vez que el Kremlin había dejado en entredicho la posición de Clinton mediante las constantes filtraciones de emails, su armada de *trolls* se dedicó a difundir otro tipo de mensajes. A partir de octubre, la finalidad pasó a ser que la sociedad estadounidense creyera que las elecciones iban a ser amañadas, y que no podían confiar en su propio sistema electoral. Una vez más, se puede apreciar el interés que tiene Putin de restarle credibilidad a las democracias liberales occidentales, haciéndoles parecer sistemas corruptos. Los *trolls* se encargaron de que se difundiera velozmente el rumor de que Clinton ya había ganado las elecciones y que no había nada que hacer. A pesar de que no hubiera evidencia alguna de ello, la teoría conspiratoria que circulaba por las redes sociales fue objeto de atención en los discursos de Trump del mes de octubre. Al entonces candidato republicano le convenía que la sociedad estadounidense creyera que Clinton había amañado las elecciones, al Kremlin le convenía que Clinton no ganara y, de no funcionar esta estrategia, sería más fácil interferir en la política de un presidente cuya victoria sería considerada por parte de la población como ilegítima. Rusia salía ganando en cualquiera de los casos (Watts, 2018, p.152).

Esta estrategia recibió apoyo, especialmente, de la prensa sensacionalista de dos países: Canadá y Macedonia. Sin embargo, los medios de comunicación en los que

aparecieron dichas noticias fueron encasillados como *clickbait*, estrategia que consiste en emitir titulares sensacionalistas cuyo único objetivo es llamar la atención del lector, con el fin de que haga clic en un enlace que o bien exagera o bien engaña directamente. Las frases empleadas para que los usuarios caigan en este ciber anzuelo son del estilo siguiente:«¡Te sorprenderá lo que te espera tras este enlace!», «¡El secreto mejor guardado, al descubierto!», «¡Ni te imaginas lo que ocurrió cuando...!» (Fundéu BBVA, 2016).

La actividad de los *trolls* aumentó en intensidad cuando finalizó la jornada de primarias y comenzaron los debates, cara a cara, entre Clinton y Trump. Durante los dos últimos meses, se observó un comportamiento que encajaba con la estrategia rusa que este trabajo ha ido exponiendo. El primer debate generó una enorme actividad en redes sociales como Twitter. Parecía que Trump contaba con una gran aprobación popular y que cada vez eran más numerosos los *tweets* de apoyo al entonces candidato. Sin embargo, el aumento de *tweets* favorables hacia el republicano fue objeto de estudio durante el siguiente debate. Una investigación realizada por expertos de la informática de la Universidad de Oxford concluyó que más de un tercio de los tweets que apoyaban a Donald Trump procedían de cuentas automáticas, lo que hace aún más sospechosa la situación que tuvo lugar durante el tercer debate, en la que tan solo uno de cada siete tweets apoyaban a Hillary Clinton (Kollanyi, Howard y Woolley, 2016)[9].

Los medios de comunicación rusos, como RT y Sputnik, colaboraron con la estrategia explicada. No obstante, dichos medios no se limitaron a publicar noticias favorables a un candidato u otro. Fueron más allá, sembrando en ocasiones el pánico. El 30 de julio de 2016 ambas agencias comenzaron a publicar una serie de artículos relacionados con una situación de descontrol en la base aérea estadounidense de Incirlik, Turquía. Dichas noticias afirmaban que se había producido un aumento en las fuerzas de seguridad turcas, bajo riesgo de un segundo golpe militar turco y de que las armas nucleares estadounidenses estuvieran en peligro. Nada más publicarse dichas noticias, Twitter estaba revolucionado, proliferando por segundos los tweets que alarmaban de un posible ataque en la base aérea, y los más catastrofistas temiendo que las armas nucleares causaran una catástrofe. Sin embargo, la prensa estadounidense se mantuvo completamente al margen de dichas afirmaciones, causando un gran desconcierto a la población. Analistas como Clint Watts, comprobaron que los tweets

[9] Ver anexo 4

que contenían el *hashtag* Incirlik eran retweeteados durante los primeros 90 minutos por cuentas en cuyas biografías aparecían, constantemente, descripciones que contenían palabras como "país, conservador, cristiano, Dios, militar" y rezaban para que este "conflicto" se solucionara lo antes posible. Como primera aproximación, dichas cuentas encuadraban a la perfección en el usuario que se corresponde con el prototipo de votantes de Donald Trump. Sin embargo, al analizar dichas cuentas, que se repetían como amplificadores de repercusión de las noticias emitidas por RT y Sputnik, se descubrió que eran falsas. No obstante, cuando este análisis concluyó era tarde. Rusia había conseguido su objetivo: alimentar el miedo que Trump estaba empleando como instrumento para que los votantes pensaran que la seguridad del país estaba en riesgo con un presidente demócrata.

3. CONCLUSIÓN:

El orden internacional ha cambiado, pero el afán de poder de las distintas potencias políticas no ha cesado en absoluto. El objetivo del Kremlin es devolver a Rusia su estatuto de gran potencia, mediante la extensión de zonas de influencia. Esto lleva a la inevitable competición con EEUU y la UE en las diferentes esferas internacionales. Sin embargo, las tendencias bélicas han dado paso a un tipo de guerra híbrida. Durante los últimos años, Rusia ha demostrado que está capacitada para desarrollar simultáneamente operaciones tanto militares como la llamada guerra de la información. Mientras que en Ucrania y Siria el gobierno ruso ha combinado ambas técnicas, en los países occidentales ha centrado su objetivo principal en ganar influencia, en lugar de territorios.

Las nuevas amenazas que componen la guerra híbrida han supuesto el surgimiento de nuevos términos, como la guerra de la información, las llamadas *Fake News*, la desinformación y la expansión en política de la llamada diplomacia pública, que puede ser definida como el intento de un actor, no necesariamente estatal, de gestionar el entorno internacional mediante el compromiso con un público extranjero, con el fin de gestionar la percepción de una determinada idea. Esta estrategia suele fijar un objetivo concreto o *target:* un conjunto de individuos dentro de un público determinado, que a su vez tienen cierta capacidad de influencia en su entorno. Dicho *target* suele consistir en un público extranjero y la finalidad es cambiar el enfoque o percepción que tenga la opinión pública sobre una idea o la imagen de un actor internacional determinado. Actualmente, la diplomacia pública es un elemento importante de la política exterior de

los Estados (Cull, 2009). A pesar de que este término ha experimentado una serie de transformaciones, el objetivo sigue siendo la gestión del entorno internacional[10].

Sin duda, la solución a este conflicto es difícil y controvertida, dado que cada actor internacional tiene una percepción distinta del mismo. Al fin y al cabo, el daño físico que realiza un arma es un dato objetivo. Sin embargo, el daño capaz de producir un arma que juega con la psicología de la opinión pública no es tan fácil de estimar. El consenso internacional acerca de esta amenaza es prácticamente inexistente. A título de ejemplo, este trabajo ha tomado como caso de estudio las elecciones presidenciales de EEUU de 2016. Uno de los documentos utilizados ha sido la citada denuncia interpuesta por el fiscal Robert Swan Mueller III contra las injerencias rusas de dicho año. El fiscal publicó un informe en el que relataba las conclusiones obtenidas de la investigación realizada, que dio lugar a la interposición de tal denuncia. No obstante, dicho documento ha sido muy controvertido. De hecho, Donald Trump ha intentado por todos los medios deslegitimarlo. El presidente de EEUU ha calificado a la investigación del fiscal como traición. Mientras tanto, Russia Today se dedica a publicar noticias que incitan a su público a no creer en dicho informe[11]. Sin embargo, este supuesto reafirma aún más las alarmantes advertencias del informe realizado por el Comité de Asuntos Exteriores del Senado de EEUU, también empleado en este trabajo para analizar el caso de estudio seleccionado. En la exposición de motivos de dicho documento, el personal que compone el comité, en el que por cierto no figura Mueller, denuncia que "el Presidente de los Estados Unidos sigue negando que exista una amenaza, creando un vacío de liderazgo en nuestro propio gobierno y entre nuestros socios y aliados europeos" (Committee On Foreign Relations of The USA, 2018, p.10).

Las democracias occidentales han dado importantes pasos en el ámbito de la libertad de expresión. Sin embargo, la consolidación de tal derecho ha abierto la puerta a nuevas amenazas, muy difíciles de reprimir sin vulnerar dicha libertad. Antes era necesario dar un golpe de estado para hacerse con el poder de un país. Actualmente, basta con publicar un *tweet* para desacreditar a cualquier político y poner en duda la legitimidad de un Gobierno.

La sociedad es al mismo tiempo víctima y participante de esta contienda. Sin embargo, es en nosotros mismos donde debe ser hallada la solución que combata a la

[10] Ver anexo 5.
[11] Ver anexo 6.

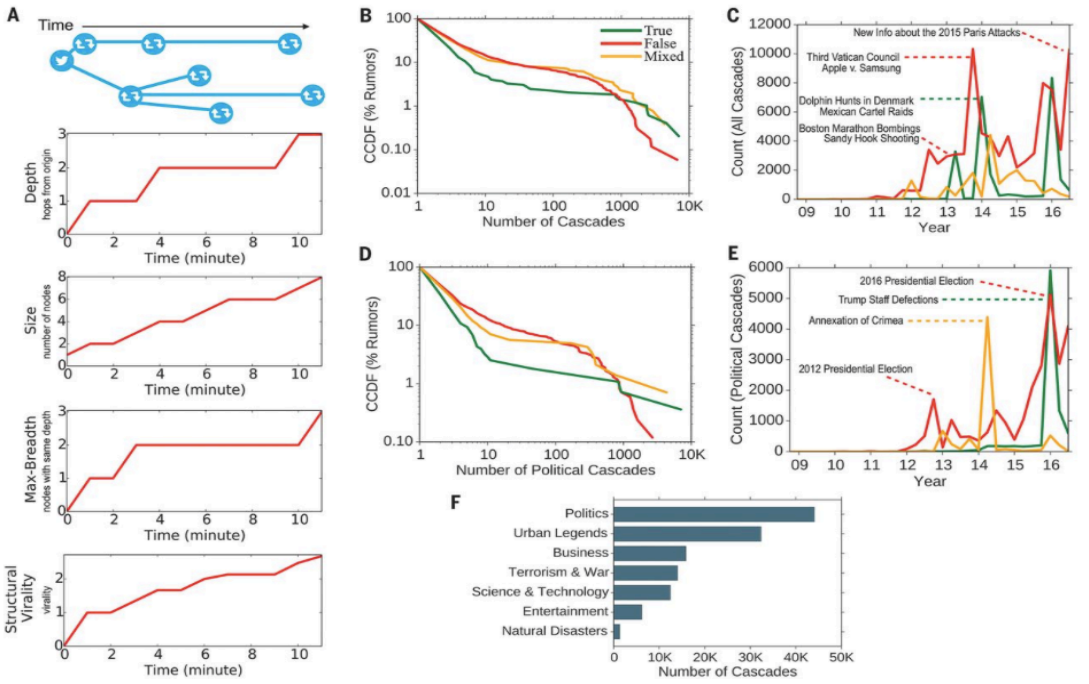
guerra de la información. Autores como Singer resaltan, en este sentido, la importancia de la educación. El motivo de ello es que, según este autor, los adolescentes son un *target* muy fácil para los medios de comunicación que, nos guste o no, forman parte de nuestro día a día. Este tipo de guerra afecta a la población más vulnerable, es decir, a la menos informada y consciente de la situación (Singer, 2018, p.261). Por ello, es fundamental crear conciencia en los colegios y universidades de la existencia de estas amenazas, enseñando a localizar una *Fake New* o un usuario que es en realidad un *troll*. Es necesario fomentar el pensamiento crítico y hacer a la sociedad conocedora de los riesgos de la desinformación, pues aunque lo ideal sería alcanzar un compromiso sólido por parte de los medios de comunicación, Mark Zuckeberg, creador de Facebook, no ha podido dejarlo más claro: los medios de comunicación no deben ser considerados árbitros de la verdad, sino meras plataformas neutrales de información (Singer, 2018, p.260). No obstante, dicha neutralidad es ilusoria y, citando a Malcolm X: "los medios de comunicación son la entidad más poderosa de la Tierra, tienen el poder de hacer culpable al inocente y al inocente culpable; y eso es poder, porque ellos controlan las mentes de las masas" (Malcolm, 1990).

Recapitulando, la guerra cibernética tan solo acaba de empezar y su intensidad no está haciendo más que aumentar. Si queremos moderar la manipulación que sufrimos día a día, el primer paso es ser consciente de ella. Los medios de comunicación no están intentando poner fin a este problema, por lo que la solución está en nosotros mismos. Debemos elegir qué papel jugamos en esta guerra, siendo conscientes de que hasta la más simple publicación que difundamos en nuestras redes sociales, puede influir en otros, moderando o fomentando la desinformación.

No obstante, no cabe duda de que se trata de un gran desafío, pues como dijo Mark Twain: "Es más fácil engañar a la gente que convencerla de que ha sido engañada" (Twain, 2013).

4. ANEXOS:

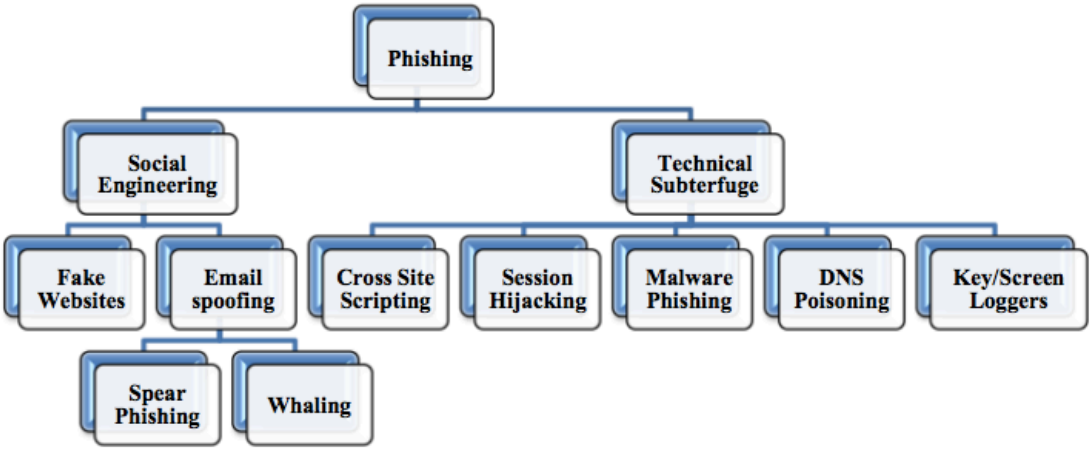
Anexo 1. Los siguientes gráficos muestran el funcionamiento de los rumores que componen las *Fake News*, caracterizadas por estar formadas por una o varias cascadas. Este último término se define como una serie de ejemplos de un patrón de propagación de rumores con un origen común. Fuente: *Science*.



El gráfico A es un ejemplo de cascada de rumores, mostrando su repercusión y tamaño en el tiempo. Los nodos representan a usuarios. El gráfico B muestra la función de distribución acumulada (CCDF) de cascadas de noticias verdaderas, falsas y mixtas (parcialmente verdaderas y parcialmente falsas), que miden la fracción de rumores que muestran un número dado de cascadas. El C y el E plasman un conjunto de recuentos trimestrales de todas las cascadas de rumores verdaderos, falsos y mixtos que se difundieron en Twitter entre 2006 y 2017. El D las CCDF de cascadas políticas verdaderas, falsas y mixtas. Por último, el gráfico F es un histograma del número total de rumores en cascada en las siete categorías temáticas más frecuentes.

Anexo 2. Recopilación de noticias publicadas por medios rusos y de denuncias contra las injerencias de los mismos. Fuente: *El País*.

Anexo 3. Tipos de ataques cibernéticos que incluye la estrategia de Phishing. Fuente: Gupta, B. B., Arachchilage, N. A., & Psannis, K. E. (2018).



Anexo 4. *Tweets* con más repercusión, publicados por los *trolls* rusos, durante la jornada preelectoral de las elecciones americanas de 2016 contra Hillary Clinton, aportados por el fiscal Robert Swan Mueller en la denuncia interpuesta ante la Corte del Distrito de Columbia, analizada en la sección referente a dicho caso de estudio. Fuente: Mueller, R. S. (2018). Indictment in The United States District Court for The District of Columbia. Case 1:18-cr-00032-DLF Doc.1.

Approximate Date	Excerpt of Advertisement
April 6, 2016	"You know, a great number of black people support us saying that #HillaryClintonIsNotMyPresident"
April 7, 2016	"I say no to Hillary Clinton / I say no to manipulation"
April 19, 2016	"JOIN our #HillaryClintonForPrison2016"
May 10, 2016	"Donald wants to defeat terrorism . . . Hillary wants to sponsor it"
May 19, 2016	"Vote Republican, vote Trump, and support the Second Amendment!"
May 24, 2016	"Hillary Clinton Doesn't Deserve the Black Vote"
June 7, 2016	"Trump is our only hope for a better future!"
June 30, 2016	"#NeverHillary #HillaryForPrison #Hillary4Prison #HillaryForPrison2016 #Trump2016 #Trump #Trump4President"
July 20, 2016	"Ohio Wants Hillary 4 Prison"
August 4, 2016	"Hillary Clinton has already committed voter fraud during the Democrat Iowa Caucus."
August 10, 2016	"We cannot trust Hillary to take care of our veterans!"
October 14, 2016	"Among all the candidates Donald Trump is the one and only who can defend the police from terrorists."
October 19, 2016	"Hillary is a Satan, and her crimes and lies had proved just how evil she is."

Anexo 5. Comparación entre la antigua diplomacia pública y la concepción teórica actual de este mismo término. Se empezó a hablar de nueva diplomacia pública a partir del año 2005. Fuente: Cull, N. J. (2009). *Diplomacia pública: consideraciones teóricas*.

Cuadro 1
La antigua diplomacia pública y la nueva

Características predominates	**Antigua diplomacia pública**	**Nueva diplomacia pública**
1. Identidad del actor internacional	Estado	Estado y no Estado
2. Entorno tecnológico	Radio onda corta, periódicos impresos, teléfonos de línea fija	Satélite, Internet, noticias en tiempo real, teléfonos móviles
3. Entorno de los medios	Línea clara entre esfera de noticias nacional e internacional	Difuminación de las esferas de comunicación nacional e internacional
4. Fuente de enfoque	Desarrollo de la teoría de defensoría y propaganda políticas	Desarrollo de la teoría de denominación y redes corporativas
5. Terminología	"Imagen internacional", "prestigio"	"Poder blando", "denominación nacional"
6. Estructura del rol	Vertical, de actor a población extranjera	Horizontal, facilitada por el actor
7. Naturaleza del rol	Mensaje dirigido a objetivo	Construcción de relaciones
8. Objetivo general	*Gestión del entorno internacional*	*Gestión del entorno internacional*

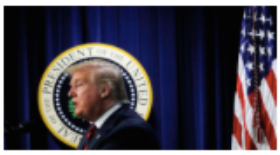
Anexo 6. Tan solo algunas de las noticias que aparecen en la página web de Russia Today cuando se teclea en su buscador "Informe Mueller", documento que denunciaba la injerencia rusa durante las elecciones estadounidenses de 2016. Puede observarse cómo este medio insistió en difundir un mensaje determinado: que tal informe no era cierto. Estas noticias fueron publicadas entre el 18 y el 19 de abril de este mismo año, con un intervalo de horas entre ellas suficiente para conseguir alcanzar al receptor.

Trump asegura que las elecciones presidenciales de 2016 "no se vieron afectadas" por la injerencia rusa

El mandatario de EE.UU. ha escrito en su cuenta de Twitter que los comicios no se vieron afectados por Rusia.

18 abr 2019 | 23 : 48 GMT 1541
https://actualidad.rt.com/actualidad/312171-trump-asegura-elecciones-presidenciales-2016

"¡Acoso presidencial!": Trump arremete contra el "mayor engaño político" antes de la publicación del informe Mueller



El fiscal general de EE.UU. hará pública este jueves una versión editada del informe del fiscal especial sobre la presunta colusión de Trump con Rusia durante las elecciones presidenciales de 2016.

18 abr 2019 | 12 : 54 GMT 20127
https://actualidad.rt.com/actualidad/312112-acoso-presidencial-trump-arremeter-infiorme-mueller

"Game over": Trump reacciona a la ausencia de pruebas de su 'colusión' con Rusia al estilo de 'Juego de Tronos'

La investigación del fiscal especial Robert Mueller sobre la presunta colusión de Donald Trump con Moscú durante las elecciones presidenciales de 2016 concluyó sin que se hallaran evidencias de la misma.

18 abr 2019 | 14 : 09 GMT 11247
https://actualidad.rt.com/actualidad/312119-trump-colusion-rusia-game-over

Periodista: "Hay una carga política muy fuerte" en la pesquisa de Mueller sobre la trama rusa

El periodista Pedro González Munné estima que en la investigación del fiscal especial estadounidense Robert Mueller sobre la presunta colusión de Donald Trump con Rusia durante las elecciones presidenciales que Estados Unidos celebró en 2016 "hay una carga política muy fuerte". Al mismo tiempo, este analista recalca que el ruido mediático relacionado con esa pesquisa elevó falsas expectativas en torno a su desenlace.

18 abr 2019 | 18 : 49 GMT 324
https://actualidad.rt.com/video/312148-periodista-carga-politica-fuerte-pesquisa-mueller-trama-rusa

5. BIBLIOGRAFÍA

Alandete, D. (2018). RT, Sputnik y la nueva guerra rusa. *El País*. Obtenido el 15/03/2018 de https://elpais.com/politica/2017/12/31/actualidad/1514736685_318060.html.

Baños, P. (2017). *Así se domina el mundo: desvelando las claves del poder mundial*. Ariel.

Barbé, E. (1987). El papel del realismo en las relaciones internacionales (La teoría política internacional de Hans J. Morgenthau). *Revista de Estudios Políticos*, (57), 149-176.

Bennett, G. (2000). The Federal Security Service of the Russian Federation. *Conflict Studies Research Centre, Royal Military Academy Sandhurst*.

Chen, A. (2015) The Agency. *The New York Times*. Obtenido el 12/02/2019 de https://www.nytimes.com/2015/06/07/magazine/the-agency.html

Committee on Foreign Relations of The United States Senate (2018). Putin's Asymmetric assault on democracy in Russia and Europe: Implications for U.S. National Security . *U.S Government Publishing Office*. Obtenida el 12/01/2019 de http://www.gpoaccess.gov/congress/index.html.

Contreras, F. R. (2004). *Culturas de guerra: medios de información y violencia simbólica*. Madrid: Anaya.

Cull, N. J. (2009). *Diplomacia pública: consideraciones teóricas*. Buenos Aires: SRE.

Dave, P. y Stubbs, J. (2017) Russia Vows Retaliation Against Google If Sputnik, RT Get Lower Search Rankings *Fortune.Com*, 1. Obtenido el 17/03/2019 de

http://search.ebscohost.com/login.aspx?direct=true&db=bth&AN=126354491&lang=es&site=eds-live&scope=site.

Eissa, S. G. (2011). Guerra hibrida ¿una nueva forma de pensar la guerra en el siglo XXI. *Researchgate*. Obtenido el 15/02/2019 de https://www.researchgate.net/profile/Sergio_Eissa/publication/268200629_guerra_hibrida_una_nueva_forma_de_pensar_la_guerra_en_el_siglo_xxi/links/5acbabe9aca272abdc63655c/guerra-hibrida-una-nueva-forma-de-pensar-la-guerra-en-el-siglo-xxi.pdf

English, R. D. (2017). Russia, Trump, and a New Detente. *Foreign Affairs*.

Fukuyama, F. (1992). *El fin de la historia y el último hombre*. Barcelona: Planeta.

Fukuyama, F. (1999). Pensando sobre el fin de la historia diez años después. *El País*, *17*(06).

Fundéu BBVA (2016). Ciberanzuelo», la alternativa favorita de nuestros seguidores a clickbait. *Noticias del español*. Obtenido el 27/ 01/ 2018 de https://www.fundeu.es/noticia/ciberanzuelo-la- alternativa-favorita-de-nuestros-seguidores-a-clickbait/.

Gianvecchio, S., Wang, H., & Jajodia, S. (2010). Who is tweeting on Twitter: human, bot, or cyborg?. In *Proceedings of the 26th annual computer security applications conference*, 21-30.

Gupta, B. B., Arachchilage, N. A., & Psannis, K. E. (2018). Defending against phishing attacks: taxonomy of methods, current issues and future directions. *Telecommunication Systems*, 67(2), 247-267.

Hobbes, T. (2006). *Leviathan*. Critical Edition by J. Rogers and Karl Shuhmann. Londres: A&C Black.

Hoffman, F. (2007). *Conflict in the 21th century: the rise of Hybrid Wars*. Arlington: Potomac Institute for Police Studies.

Howard, P. N., & Kollanyi, B. (2016). Bots, StrongerIn, and Brexit: computational propaganda during the UK-EU referendum. Obtenido el 21/01/2019 de https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2798311

Huntington, S. P. (1997). El Choque de Civilizaciones. Buenos Aires: Paidos.

IEEE International Conference on Big Data(2016). Identifying trolls and determining terror awareness level in social networks using a scale framework. *IEE International Conference On Big Data*. Obtenido el 05/03/2019 de https://doi.org/10.1109/BigData.2016.7840796

Indiana University Information Technology Services (2008). What is a troll?. *Indiana University Knowledge Base*.

International Institute for Strategic Studies. (2017). Military Balance 2017.

Ioffe, J. (2010). What Is Russia Today?. *Columbia journalism review*, *49*, 44-49.

Keohane, R. O. (2005). *After hegemony: Cooperation and discord in the world political economy*. New Jersey: Princeton University Press.

Khatchadourian, R. (2010). No secrets. Julian Assange's mission for total transparency. *New Yorker*, *7*.

Kollanyi, B., Howard, P. N., & Woolley, S. C. (2016). Bots and automation over Twitter during the third US presidential debate. *Project on Algorithms, Computational Propaganda, and Digital Politics*.

Lieven, A. (1999). *Chechnya: tombstone of Russian power*. New Haven: Yale University Press.

Malcolm, X. (1990). *Malcolm X speaks: Selected speeches and statements* (Vol. 125). Grove Press.

Marcus, S. (1982). Actualidad de Orwell. *Revista de Occidente*, 1, 65-80.

Microsoft. (2009). Virtual Private Networking: An Overview. Obtenido el 15/02/2019 de https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-2000-server/bb742566(v=technet.10.

Minchenko Consulting Communication Group (2016), *Vladimir Putin's Big Government and the Politburo 2.0.,* Obtenido el 10/01/2019 de http://minchenko.ru/netcat_files/File/Big%20Government%20and%20the%20Politburo%202_0.pdf

Milosevich-Juaristi, M. (2017). La "combinación", instrumento de la guerra de la información de Rusia en Cataluña. *Real Instituto Elcano,* 86. Obtenido el 12/03/2019 de http://www.realinstitutoelcano.org/wps/portal/rielcano_es/contenido?WCM_GLOBAL_CONTEXT=/elcano/elcano_es/zonas_es/ari86-2017-milosevichjuaristi-combinacion-instrumento-guerra-informacion-rusia-cataluna

Morales Hernández, J. (2003). Los servicios de seguridad e inteligencia en la Rusia de Putin. *UNISCI Discussion Papers*, (2).

Morgenthau, H. J. (1986). *Política entre las naciones: la lucha por el poder y la paz*. Buenos Aires: GEL.

Mueller, R. S. (2018). Indictment in The United States District Court for The District of Columbia. Case 1:18-cr-00032-DLF Doc.1. Obtenida el 13/01/2019 de https://www.justice.gov/file/1035477/download.

Murillo de la Rocha, J. (2005). La disolución del imperio soviético y los nuevos desafíos del mundo actual. *Revista Ciencia y Cultura*, 17, 91-105.

Paul, C., & Matthews, M. (2016). The Russian "firehose of falsehood" propaganda model. *Rand Corporation*, 2-7. Disponible en: http://www.intgovforum.org/multilingual/sites/default/files/webform/RAND_PE198.pdf

Pauselli, G. (2013). Teorías de relaciones internacionales y la explicación de la ayuda externa. *Iberoamerican Journal of Development Studies*, *2*(1), 72-92.

Perry, T. (2018). I was a Russian troll named Martha, *IEEE Spectrum*, 6 (6) Obtenido el 01/02/2019 de https://doi.org/10.1109/MSPEC.2018.8362210.

Pizzonia, C. (2018). *La (In) Evitabilidad De La Disolución De La Urss. Un Análisis De Causas Y Consecuencias*. México: Itaca.

Popken, B., & Cobiella, K. (2017). Russian troll describes work in the infamous misinformation factory. *NBC*. Obtenido el 18/02/2019 de https://www.nbcnews.com/news/all/russian-troll-describes-work-infamous-misinformation-factory-n821486

Richardson, B. (2018). Our Party: Who we are. Obtenido el 14/02/2019 de https://web.archive.org/web/20120120111331/http://www.democrats.org/about/our_party.

Rodríguez, R. (2013). Hacia un estado de la cuestión de las investigaciones sobre desinformación/misinformación. *Correspondencias & análisis*, 319-342.

Romero, L. (2012). La desinformación en la nueva aldea global. *Comunicación. Estudios venezolanos de la Comunicación*, *159*, 52-55.

Singer, P. W., & Brooking, E. T. (2018). *LikeWar: The Weaponization of Social Media*. Nueva York: Eamon Dolan Books.

SIPRI Yearbook: Armaments, Disarmament and International (2018). Stockholm International Peace Research Institute. Obtenido el 12/03/2019 de https://sipri.org/sites/default/files/2018-08/yb18_summary_esp.pdfe

Twain, M. (2013). *Autobiography of Mark Twain*. University of California Press.

Uchill, J. (2016). Typo led to Podesta email hack: Report. *The Hill*. Obtenido el 03/01/2019 de https://thehill.com/policy/cybersecurity/310234-typo-may-have-caused-podesta-email-hack

Waltz, K. (1959). *El hombre, el Estado y la guerra*. Buenos Aires: Nova.

Watts, C. (2018). *Messing with the enemy: Surviving in a social media world of hackers, terrorists, Russians, and fake news*. Nueva York: Harper Business.

Weir, F. (2010). WikiLeaks ready to drop a bombshell on Russia. But will Russians get to read about it?. *The Christian Science Monitor (Boston)*.Obtenido el 23/01/2019 de http://www. csmonitor. com/World/Europe/2010/1026/WikiLeaks-ready-to-drop-a-bombshellon-Russia.-But-will-Russians-get-to-read-about-it

WikiLeaks: Hillary Clinton Email Archive. (n.d.). Obtenido el 12/02/2019 de https://wikileaks.org/clinton-emails/.

Wolton, D. (1992). *War game: la información y la guerra*. Madrid: Siglo XXI.

Woolley, S. C., & Howard, P. N. (2017). Computational propaganda worldwide: Executive summary. *Working Paper* on Projecton Computational Propaganda.

Yang, C. y Yuan, J. (2018). Construction of Culture Soft Power and a Community of Shared Future. *Revista de Cercetare Si Interventie Sociala, 63, 54-69*.