LA GUERRA DE DES-INFORMACIÓN DE RUSIA EN ESTADOS UNIDOS

Omar Villota Hurtado[6]

RESUMEN

Este documento contiene un recuento de las operaciones de influencia de Rusia en la elección presidencial norteamericana del 2016. De manera que el objetivo del texto es presentar observación y análisis académico, contrastadas con las teorías de comunicación, evidencias y pruebas de contra inteligencia ante la seguridad nacional con base en los reportes de ciberseguridad luego de ataques persistentes a sistemas informáticos de muy variadas instituciones de Estados Unidos.

Como método de investigación documental se usó el testimonio de fuentes primarias expresado ante el Comité Selecto de Inteligencia del Senado (CSIS) norteamericano, recopilado en las más de diez audiencias y sesiones informativas iniciadas en 2015 y documentos oficiales desclasificados de las agencias nacionales de seguridad estadounidense. Cada sección de este texto se enmarca dentro de la crisis de legitimidad y de credibilidad del sistema liberal democrático.

Los primeros resultados examinan y entienden la escala y el alcance de las actividades rusas, que se agrupan en dos estrategias básicas: medidas activas y campañas de influencia. Los expertos han clasificado el modo de trabajar de Rusia mediante medidas

[6] Docente universitario en temas de comunicación digital y gestión del conocimiento para inteligencias colectivas.
Comunicador, especialista en redes de información documental y máster en comunicación digital con más de 25 años de experticia. Investigador sobre temas de cibercultura y tecnologías aplicadas. Trabajo en actividades de gestión de conocimiento para inteligencias colectivas. Optimizo el entorno virtual con base en emprendimiento y conocimiento disciplinar mediante estrategias, creatividad e innovación de ruptura. Autor de libros y artículos académicos para varias revistas indexadas que puede leer en http://orcid.org/0000-0003-3743-3734

activas, campañas de influencia sobre mensajes engañosos, propaganda falsa y agentes involuntarios.

De manera relevante palabras rusas como *dezinformatsia* (desinformación), *aktivniye meropriyatiya* (medidas activas), *kompromat* (material comprometedor) y *kombinatzia* (empleo de técnicas tanto abiertas como encubiertas) ingresaron al léxico de los círculos políticos y académicos de Norteamérica, porque según los expertos la seguridad está amenazada por la "guerra híbrida", sobre todo.

PALABRAS CLAVE

Ingeniería social, Información política, Desinformación social, Medios electrónicos.

SUMARIO

Se analiza lo ocurrido en materia de medidas activas y campañas de influencia ejecutadas por Rusia, previo al proceso electoral que eligió al presidente número 45 en Estados Unidos en el año 2016, dentro del contexto teórico de la manipulación porque es la práctica de la interacción comunicativa del discurso político. La manipulación comprende abuso del poder que significa dominación.

Manipular el discurso político obviamente combina formas de influencia ilegítima pero una sutil diferencia decisiva es la práctica legítima que defienden los políticos, sustentada en la racionalidad argumental. Se trata de la persuasión, donde los interlocutores son libres de creer o de actuar según les plazca y acepten o no los argumentos del otro.

La consecuencia negativa al manosear el discurso político rebasó a los electores -gratificados al rol pasivo- quienes enfrentaron las tesis políticas de Hillary Clinton y Donald Trump. Fueron pasivos al no poseer habilidad para comprender las reales intenciones del manipulador –no solo los grupos de hacker de Rusia sino Wikileaks, Twitter y Periodistas-;

carecieron del conocimiento específico para deliberar libremente con base en los mensajes -que desacreditaban y socavaban a líderes e instituciones democráticas, que debilitaban la confianza de los mercados financieros y las empresas capitalistas, que ampliaron las divisiones destruyendo la confianza ciudadana y que incitaban al miedo del cambio climático catastrófico-; no resistieron la confabulación y terminaron siendo víctimas en un enfoque triangulado -social (involucra interacción y abuso de poder entre grupos políticos y actores sociales), cognitivo (implica manipulación de mentes de los participantes) y discursivo (contiene mensajes oral, escrito y visual)-.

INTRODUCCIÓN

Los sustantivos "guerra" y "desinformación" que utilizo en el título de este documento gravitan en torno al problema evidente, real, sin mezcla, que afecta el sentido de la responsabilidad moral e intelectual. Su aparición consecuente enmarcó el plan sistemático de la presencia de Rusia en el proceso electoral de Estados Unidos del año 2016, que desestabilizó a las instituciones democráticas.

Una evidencia inicial es la investigación de Vosoughi, Roy & Aral acerca de la difusión de distintas noticias verdaderas, falsas y mixtas (parcialmente verdaderas y falsas) difundidas por Twitter en inglés durante el periodo 2006 hasta 2017[7]. Ellos analizaron el mensaje, la etiqueta y precisaron en tres niveles el dictamen -verdadero, falso o mixto- en cada rumor informado por sitios web y recolectado automáticamente en la plataforma social Twitter. El resultado sigue siendo alarmante. Un extracto del resumen (Vosoughi, Roy, & Aral, 2018) explica que:

> A medida que se retweet un rumor, la profundidad (el número de saltos a lo largo del tiempo del retweet a partir del tweet original), tamaño, amplitud máxima y viralidad estructural aumentan en la línea de tiempo. Se evidenció que una fracción mayor de rumores falsos lograron entre una y mil cascadas (una medida interpuesta entre el contenido de una única transmisión grande que se propaga a través de la

[7] Los datos incluyeron alrededor de 126.000 rumores difundidos por más o menos 3 millones de personas que *retweet* más de 4.5 millones y que fueron verificadas por las organizaciones independientes de *fact-checking*: snopes.com, politifact.com, factcheck.org, truthorfiction.com, hoax-slayer.com y urbanlegends.about.com

distribución de múltiples generaciones, donde cualquier persona es directamente responsable de la difusión de un segmento o del total del mensaje) en siete temas: política, leyenda urbana, negocio, terrorismo y guerra, ciencia y tecnología, entretenimiento y desastre natural. También fue verdadero el testimonio de encontrar mayor cantidad de retweet para rumores basados en noticias políticas.

La cantidad total de rumores falsos llegó a un punto máximo (más de 100.000 cascadas) al final del año 2013 con el tema tercer consejo vaticano y muy por debajo (unas 70.000 cascadas), se ubicaron las noticias verdaderas sobre la caza de delfines en Dinamarca y las incursiones de los carteles mexicanos de narcotráfico. Nuevamente a fines del año 2015 por el tema de los atentados a París, la cota de rumores falsos alcanzó el máximo de la del año 2013. Los datos recogidos en la investigación de Vosoughi, Roy, & Aral también muestran crecimientos en el número total de rumores falsos de tema político (cerca de 20.000) durante las elecciones presidenciales de Estados Unidos del año 2012, entre el demócrata Barack Obama y el republicano Mitt Romney, y más de 2,5 veces más altos para el año 2016 cuando ganó el republicano Donald Trump. En el lapso de las publicaciones sobre la anexión rusa de Crimea del 2014 se observa un aumento en los rumores mixtos de unos 45.000. En síntesis, mientras el tema político (por encima de 45.000 cascadas) fue la categoría de rumores más grande en esos datos los aspectos de entretenimiento y desastres naturales fueron los de menor rumor (ambas por debajo de 7.000). Las demás categorías de rumores tuvieron estas propagaciones: leyendas urbanas (más de 30.000), negocios (unos 17.000), terrorismo (alrededor de 15.000) y ciencia y tecnología (unos 13.000).

Desde la perspectiva académica, el teórico Teun van Dijk, analista crítico del discurso, ha argumentado que la manipulación –como forma simbólica o comunicativa- involucra el abuso del poder y la dominación que este genera (van Dijk, 2006). Su expresividad dentro del lenguaje implica el ejercicio de un modo del discurso de influencia ilegítima, pues los manipuladores son especies de magos que influencian la creencia de los otros para que hagan cosas favorables al manipulador, pero perjudiciales para el manipulado. De manera que un discurso manipulativo en sentido semiótico puede ser ejercido mediante

iconografías, fotos, películas u otros medios que se distribuyen dentro de un contexto social.

Al ejercer cierta influencia en las creencias de las personas es natural que se trata de un control de la mente acompañado si y solo sí por la dominación de las acciones que aplica el receptor del mensaje comunicativo. De allí que sean más los *new media* los mayores proclives a satisfacer ciertos criterios personales y sociales lo que les permite a los manipuladores influir sobre otros. Considerando que los *mass media* se nutren del contenido ciudadano y de redes digitales, la ética periodística enseña que los medios de comunicación también contraen deudas con toda la sociedad "debido a que existe un poder pedagógico en la información pública que los medios pueden potenciar... y le crean al periodista deberes como el de mantener activa una mirada crítica sobre los hechos y personas que influyen" (Restrepo, 2016).

Una práctica manipuladora en la comunicación política enmarca ciertas condiciones sociales para ese control. Por ejemplo, la formulación del discurso debe expresarse en términos de pertenencia del grupo, de la posición institucional, de la profesión, de los recursos materiales o simbólicos, entre otros elementos que definen el poder de los miembros del grupo emisor. De manera que la manipulación comunicativa se ha convertido en compleja desinformación dado el lenguaje habitual de políticos y periodistas. En lo gramatical, el término desinformación introducido en el diccionario por la Real Academia Española solo hasta el año 1992 presenta dos acepciones: 1. Dar información intencionadamente manipulada al servicio de ciertos fines y 2. Dar información insuficiente u omitirla. Diez años atrás el diccionario *Larousse* lo había incluido por primera vez como "acción de suprimir información, de minimizar su importancia o de modificar el sentido" (Jacquard, 1988, pág. 9).

Como estrategia política la desinformación y otras operaciones de influencia más amplias a la que irradian los *mass media* han sido ejecutadas adrede en internet por grupos de hacker. Por ejemplo, algunos de Rusia emprendieron procedimientos para la elección presidencial norteamericana del año 2016. Aquella información insuficiente e intencionadamente manipulada estaba ya inserta en las tácticas militares Bolcheviques

denominadas *activniye meropriyatya* (medidas activas). Los teóricos Shultz & Godson argumentan que mediante la destreza de la desinformación la Rusia soviética tenía como objetivo principal "desacreditar, debilitar a los oponentes y distorsionar su percepción de la realidad" (Shultz & Godson, 1984, pág. 2). Así mismo, (Sokolovsky, 1981) arguye que las medidas activas fueron los pilares para cumplir dicha estrategia militar soviética. Desde la academia, Arribas & Barberá exponen que, con base en la "Teoría de los Efectos, desde la perspectiva de la propaganda, en la Rusia Soviética surgida a partir de la Revolución Bolchevique de 1917… la comunicación política jugó un papel preponderante… como persuasión de masas, así como creación de opinión pública" (Arribas & Barberá, 2018, pág. 50). Aquellas medidas activas conformarían entonces una colección de desinformación mediante acciones, según la catalogación de las técnicas de desinformación que efectúo García-Avilés (La Desinformación, 2009).

En la actualidad, para Romero-Rodriguez la pragmática de la desinformación orienta situaciones pre-comunicativas como la sobresaturación, llegando a límites de la asimilación cognitiva, la media-morfosis y la ecología de la información (Romero-Rodriguez, 2014, págs. 19-53), cuya producción informativa se focaliza según las condiciones políticas y económicas, las industrias comunicativas, la organización productiva mediática y las estrategias discursivas de los productos informativos.

En el marco de este reportaje sobre las operaciones de influencia de Rusia al momento de la elección presidencial norteamericana del año 2016, las medidas activas que provenían del régimen soviético de preguerra se explayaron en estrategias digitales, sobre todo, a través de la desinformación (*dezinformatsia*), del material comprometedor (*kompromat*) y del empleo de técnicas tanto abiertas como encubiertas (*kombinatzia*). Estos términos hubieron de ser apropiados por la inteligencia y la Academia de Norteamérica como nuevo léxico siendo insertado en el concepto de propaganda, provocación, manipulación de extranjeros, infiltración de agentes y operaciones paramilitares encubiertas. Dice Rodríguez Andrés, citando a Cathala, que…

> el fenómeno no es esencialmente innovador, aunque lo que sí es reciente es el término concreto para denominarlo… en una situación histórica muy específica, caracterizada por: la lucha constante entre Estados Unidos y la Unión Soviética, que llevó a ambos países a perfeccionar sus métodos de espionaje y de ataque al rival. Y el avance y desarrollo de los modernos medios de comunicación, cuyo poder de difusión fue utilizado por ambas potencias para influir en el público (Rodríguez Andrés, 2018, pág. 234).

El modo de afrontar esta investigación se lleva a cabo a través de mapear los testimonios de fuentes primarias expresados en el Comité Selecto de Inteligencia del Senado (SSCI), célula legislativa estadounidense que investigó la visión de la defensa de Rusia para ejecutar un socavamiento al sistema político, económico y social de Occidente mediante mensajes falsos, verdaderos, engañosos, desinformados, dirigidos a los receptores de redes digitales, en especial justo para el proceso electoral que elegía al presidente 45 de Estados Unidos en el año 2016. El contraste a las fuentes primarias de información es una habilidad que se enseña, en especial, en el periodista "aunque cambien los canales y las herramientas", dice Ernesto Villar, Doctor en Periodismo del Centro Universitario Villanueva, siendo "realista verificar la información antes de publicarla porque ese es uno de los elementos constitutivos del periodismo. De lo contrario, seremos replicantes o altavoces. No periodistas", sustenta Xosé López, Profesor de Periodismo en la Universidad de Santiago de Compostela, por cuanto "tenemos que ser cautos y no dar crédito a una información de la que desconocemos su origen. La credibilidad es el único patrimonio que tiene un periodista", según lo expresa Juan Pablo Bellido, Profesor del Campus Universitario EUSA, centro adscrito a la Universidad de Sevilla (Reasonwhy, 2018).

Para julio del año 2016, tan solo cuatro meses previos a las elecciones presidenciales norteamericanas, celebradas el martes 8 de noviembre, los medios de comunicación rusos habían asumido la New Generation Warfare (NGW: Guerra de Nueva Generación). Es una estrategia de influencia, no de fuerza bruta, según la indagación de Milosevich-Juaristi y que para Dimitri Kiselyov - director de la agencia Russia Today

(*Rossiya Segodnaya*) y de una de las televisiones estatales (VGTRK)- "…hoy en día es mucho más costoso matar el soldado de un ejército enemigo que en la Primera o en la Segunda Guerra Mundial y si puedes persuadir a una persona, no hace falta matarla (MacFarquhar, 2016). En lo académico, Sergio Príncipe Hermoso, Profesor de Periodismo de la Universidad Complutense de Madrid, señala que "el escándalo en Estados Unidos de las presuntas injerencias de Rusia en la campaña electoral que dio la victoria a Donald Trump o en Europa, el 'brexit' y la situación de Cataluña… son buena prueba de que los más vulnerables son los jóvenes" (Reasonwhy, 2018).

Las evidencias

Desde 1920 existen algunos vocablos en idioma ruso que fueron menospreciados inicialmente por las agencias de seguridad nacional de Estados Unidos. Definían las tácticas abiertas y encubiertas (*kombinatzia*) para llevar a cabo operaciones de inteligencia soviética. En el siglo 21 se siguen relacionando con dos estrategias, pero de los servicios de inteligencia rusos: medidas activas y campañas de influencia. Con ellas intervinieron directamente en la elección presidencial de 2016 en Estados Unidos al atacar a través de agentes las instituciones de Occidente.

Testimonios expresados por expertos en la sesión senatorial norteamericana del SSCI no solo coinciden en cuanto a las pruebas sino además en los motivos del regreso ruso a la escena mundial, terminada la Guerra Fría. Y en especial, en las razones por las cuales Moscú utiliza una amplia gama de instrumentos subversivos, muchos de los cuales no son militares, para promover sus intereses nacionales a escala global. Todos los participantes convocados a las reuniones por el Congreso norteamericano asimismo se mostraron convencidos que las intrusiones a través de actividades encubiertas cibernéticas desde grupos hacker de Rusia tuvieron el propósito de: interferir, engañar, desinformar, falsificar información abiertamente, influenciar a personajes y atacar sitios web públicos mediante la explotación del bien conocido lenguaje informático estándar Structured Query Language (SQL). En consecuencia, aquel Comité Senatorial consideró que "si bien el

alcance completo de la actividad rusa contra 21 estados de Norteamérica[8] sigue sin estar claro [para el año 2018] debido a las brechas en la recolección de datos... el Comité cree que la actividad indica un intento de ir más allá de la recopilación desde la inteligencia tradicional" (U.S. Senate Select Committee on Intelligence, 2018, pág. 1).

Este resultado estriba en las explicaciones de los testigos citados quienes rindieron convincentes análisis con respecto a la ruptura del servidor informático del Comité Nacional Demócrata (DNC), a las publicaciones de propaganda en el diario Russia Today patrocinadas por Rusia, a los innumerables mensajes de trolls que utilizaron internet para divulgar *fake news* o historias distorsionadas, a la configuración de engañosos portales web para servicios de noticias y a otros eventos de muy amplia divulgación mediática en su momento de ocurrencia. Aun así, el Comité tiene información limitada con respecto a la actividad adicional que aún no se ha descubierto.

Corrobora lo anterior Eugene Rumer, director del programa Russia and Eurasia y miembro del Fondo Carnegie for International Peace. En aquel 8 de mayo de 2018, otro día de sesiones del SSCI, aseguró que "el alcance total de la injerencia rusa en las elecciones presidenciales del 2016 todavía no se conoce públicamente" (Homeland Security Digital Library, 2018, pág. 9) pese a que, Roy Godson, Profesor Emeritus en Gobierno de Georgetown University y representante de instituciones académicas, dio a conocer el modo en que se configuran los equipos hacker: "mantienen y desarrollan un grupo de personal, tanto delatado como encubierto, convenientemente entrenado para continuar su manipulación con agentes extranjeros de influencia, y utilizan nuevas geo tecnologías que se adaptan en línea como potenciadores de fuerza" (Homeland Security Digital Library, 2018, pág. 10). Por lo general, las acciones que llevaron a cabo los equipos hacker fueron efectivas, pero otras solo generaron enfado.

Las actividades efectivas, aun cuando no tienen un plan prediseñado, identifican y buscan oportunidades de ataque en la medida que las van cruzando con todas las tácticas posibles. De manera que las encubiertas como las desveladas son una de las más antiguas

[8] Este número solo tiene en cuenta los objetivos víctimas del gobierno estatal o local, según el informe de 8 de mayo del 2018, Orientación de Rusia a la infraestructura electoral durante la elección de 2016: resumen de los hallazgos iniciales y recomendaciones. Disponible en https://www.intelligence.senate.gov/publications/russia-inquiry

combinaciones (*kombinatzia*) que se remonta a los tiempos zaristas y siguen activas para reforzar los objetivos víctimas a medio y largo plazo.

Empíricamente vivimos en un mundo de conflicto multidimensional ocasionado por diversos agentes y factores. Desde la economía oscilan entre "el cambio climático, el patriarcado y lo que eso representa como reacción violenta del machismo y del sexismo contra las mujeres, quienes han alcanzado consciencia de auto emancipación, siendo esta la crisis de mayor desigualdad humana" (Castells, 2018). Sin embargo, la más peligrosa es la crisis de legitimidad de las instituciones democráticas lo que quiere decir que sin instituciones es muy difícil gestionar todos estos problemas, ya que las instituciones solo son fuertes cuando viven en la mente de los ciudadanos (Castells, 2017).

Ante esta actual crisis global del sistema democrático liberal la sociología presenta dos líneas de análisis: la crisis de legitimidad y de confianza de dos tercios de la humanidad ante todas las instituciones y, en recíproco, el aumento del correctivo ante nuestras creencias democráticas. En la práctica entonces hay notorio surgimiento de actores políticos decisivos -Rusia y China- que, siendo capaces, imponen en las mentes de los ciudadanos un sistema de gestión autoritario, eficaz y no necesariamente tan legítimo, pero sí lo suficientemente estable.

El Entorno Virtual

Internet, *new media* y *social media platforms* -o lo que estudios en periodismo digital denominan 'ecología de medios'- son el anónimo teatro de operaciones donde se ejecuta velozmente la "guerra de información" (Weisburd, Watts , & Berger, 2016), caracterizada principalmente por la narrativa transmedia. Es decir, la historia se cuenta en muchos medios y plataformas, y el público participa difundiéndola con emotividad. El uso de la información, expresada como categoría "arma informativa", es una estrategia mediática que se viene expandiendo con fuerza en la era de la posverdad. Hay, por tanto, prevalencia ciudadana por difundir argumentos emocionales y descalificar a quien transmite tesis racionales, además de que tampoco se confía en las instituciones y se

evidencia en el individuo incapacidad para distinguir noticias verídicas de informes engañosos. Acojo la definición de noticia argumentada dada por (Vosoughi, Roy, & Aral, 2018) como "cualquier historia o reclamo que se extiende como fenómeno social a través de una afirmación y un rumor de una suceso o reclamo difundido a través de las redes".

En concreto, "Facebook y Twitter siguen llenas de cuentas pro-rusas de aspecto occidental cuyo soporte para desacreditar a Estados Unidos son los robots automatizados" (Weisburd, Watts , & Berger, 2016, págs. 1-2). El resultado de la generación y redistribución de mensajes a través del entorno virtual proporciona como verdad que "nuestras agencias gubernamentales parecen estar confundidas por los diferentes términos de protección, como respuesta a incidentes y ante la defensa nacional" (Homeland Security Digital Library, 2018, pág. 21). Con base en esta veracidad, habría la posibilidad que la información disponible para consumidores promedio pueda ser inexacta con lo que se facilita la manipulación de información.

Potencialmente la generación de rápidos rumores y exageraciones acerca de acontecimientos locales, historias particulares, amenazas nacionales y ataques cibernéticos se constituyen en embestidas sistemáticas y permanentes, siendo las más graves.

> En 2012 observé un conjunto de ataques cibernéticos destructivos realizados contra la empresa estatal de petróleo y gas Saudi Aramco, con sede central en Dhahran (Arabia Saudita), con más de 20 mil computadoras afectadas, y un siguiente ataque contra el operador global de energía de gas natural licuado, Qatari RasGas, y otros reportados contra el gobierno saudí (Homeland Security Digital Library, 2018, págs. 1-2).

Solo tres años después, en febrero de 2015, en la audiencia del Comité de Servicios Armados del Senado estadounidense, se escuchó por primera vez de ataques cibernéticos destructivos dentro del territorio de Estados Unidos. La voz de alarma fue del Director de Inteligencia Nacional, James R. Clapper, al denunciar que en

> 2014 por primera vez vi ataques llevados a cabo por entidades estado nación, contra el casino Las Vegas Sands y la corporación Sony Picture. Aunque Irán y Corea del Norte tienen capacidades técnicas menores, en comparación con Rusia y China, estos ataques destructivos demuestran otros actores cibernéticos motivados e impredecibles (Clapper, 2015, pág. 1).

Para la seguridad del sistema democracia liberal esta serie de ataques representan una tendencia vital ya que demuestran expansión en significativas capacidades cibernéticas de los estados nacionales como los mencionados: Irán, Corea del Norte, Rusia y China, e inclusive Israel. Sin embargo, no son los únicos. Hay comprobación que las acciones continuas y persistentes de los países emergentes se enmarcan en consideraciones políticas y económicas externas dirigidas a naciones que podrían estar más inclinadas a actuar en defensa del hackeo a la democracia.

Al busilis de la comunicación digital se le ha torcido el cuello y ya no es para democratizar ("horizontalizar") la información si no manipular a la sociedad pues lo detallado de la dominación, definida como abuso de poder, revela tener "control especial sobre recursos sociales escasos... como los medios de comunicación y o el discurso público… compartido por miembros de las élites simbólicas tales como políticos, periodistas, científicos, escritores, profesores…" (van Dijk, 1996, pág. 95). Internet se convierte en la red ideal para manipular a muchos mediante el texto oral, escrito o audiovisual y hasta para dar acceso a alguna forma de discurso público. "Con el nacimiento de la Internet de las cosas (IoT) y el desarrollo continuo y la rápida iteración de la tecnología es probable que las tendencias continúen acelerándose" (Alexander, 2017, págs. 1-2). Los servidores que enlaza Internet hospedan y transmiten en vivo debates parlamentarios, noticias, artículos de opinión, textos de estudio, ensayos científicos, novelas, programas de televisión, propaganda, etc. lo que constituye poder de grupo y al mismo tiempo, del discurso público con base en el acceso destinado a la reproducción social de ese poder y su control. De manera que las campañas de desinformación impulsadas por rusos en la esfera de los new media se han diseñado para quebrantar la credibilidad del gobierno de Estados Unidos.

En su investigación Weisburd, Watts, & Berger (Trolling for Trump: How Russia Is Trying to Destroy Our Democracy, 2016) han clasificado los mensajes de propaganda engañosos de Rusia en cuatro clases:

1. Mensajes políticos diseñados para empañar a líderes democráticos y socavar las instituciones democráticas.
2. Propaganda financiera creada para debilitar la confianza de los mercados financieros, las economías capitalistas y las empresas de Occidente.
3. Malestar social organizado para ampliar las divisiones entre la población democrática a fin de destruir la confianza ciudadana y el tejido social.
4. Calamidad de desaparición global para incitar al miedo como consecuencia de una guerra nuclear o del cambio climático catastrófico.

Los Perfiles Digitales

La categoría "guerra de información", actividad que proviene de grupos de hacker, es la sucesora de la llamada "guerra electrónica" iniciada por equipos militares ante el uso del espectro electromagnético. Estas unidades específicas comenzaron a surgir de manera eficiente y coordinada durante la Segunda Guerra Mundial (1939-1945) y la Guerra Fría (1947–1991), clasificando al paradigma en la cota macro -que pregunta: ¿qué puede ser entendido? - cuya causa refiere los efectos potentes, inmediatos y planificados. Actualmente los hackers constituyen un componente común del arsenal de cualquier ejército y sus trabajos han desplazado aquel paradigma hacia la era digital que extiende una de sus ramas a la sociedad informacional.

La influencia mediática negociada (desarrollada en las décadas 1970-2000) que se erige dentro del constructivismo social, manifiesta el paradigma de los efectos poderosos en donde en ciertas ocasiones, ciertos mensajes, transmitidos mediante ciertos medios, producen ciertos efectos en ciertas personas, bajo ciertas circunstancias (Abelino, 2017). Sin embargo, aquel modelo de negociación entre ofertas mediáticas y audiencias también es trasladado hacia la sociedad red como forma dominante de organización sustentada en

una estructura social compuesta por redes de información. Su ejercicio lógico opera bajo lo binario (inclusión/exclusión) y como forma social, las redes carecen de valor (besan/matan), no tienen nada de personal (subjetividad/ identidad) en lo que hacen y son propulsadas por las tecnologías de la información, características del paradigma informacionalista (Castells, 1996). De manera que los sujetos pactan consumir o no determinados contenidos y los adecuan a su propia visión de realidad, alineados con los imaginarios sociales. La sociología interpretativa se ha desbordado a las teorías del *framing*[9] y *priming*[10] semántico (McQuail, 2000) para entender la moderna comunicación de las masas.

A la luz del campo de conocimiento Comunicación, la Teoría de los Efectos de los medios es el principal paradigma en la comunicación de masas y "en el campo de la comunicación de masas, el término 'efectos de los medios' es común" (Eveland, 2003, pág. 402). Examinaré los Efectos de los *new media* con base en cómo se entiende el sujeto, qué relación guarda con la sociedad y cuál es la importancia del contexto histórico, apoyado por las declaraciones de los expertos ante las múltiples sesiones del SSCI.

Decía Watts en el año 2017 que los perfiles observados en las identidades atacantes -para la elección presidencial norteamericana del 2016-, que usaron cuentas de redes sociales, fueron *Hecklers* [personas entusiastas quienes acosan y tratan de desconcertar a otros con preguntas, desafíos o burlas] "que parecían ser europeas, de habla inglesa, pero quienes no hicieron bien su trabajo porque el patrón de agresión, persistencia, biografía, arquetipos de habla y sincronización se notaba ser antinaturales" (Homeland Security

[9] Algunos ejemplos sobre los procesos intersubjetivos de definición de la situación abordan temas mediáticos como la inmigración (Igartua, Humanes, Muñiz et al., 2004; Igartua & Muñiz, 2004; Igartua, Cheng & Muñiz, 2005; Igartua, Otero, Muñiz, et al., 2006; Muñiz, 2007); la introducción del euro (de Vreese et al., 2001); el desempeño de líderes políticos (Semetko & Valkenburg, 2000; Shah, Watts, Domke & Fan, 2002), la imagen del feminismo (Lind & Salo, 2002) y las relaciones internacionales (Park, 2003), entre otros. Citado en (Koziner, 2013).

[10] Es manifestado en pruebas de manipulación que requiere del nivel de proceso conceptual de los estímulos según el cual, aquel procesamiento de las representaciones mentales que subyace a la memoria implícita puede verse afectado por operaciones de codificación semántica, siendo apenas sensible a los cambios de las propiedades superficiales de la información. Para la psicología cognitiva básica, el proceso de los estímulos y su recuperación implícita se encuentra en función de la organización semántica (Tulving & Schacter, 1990) y de las diferentes manipulaciones experimentales dadas por la disociación entre pruebas implícitas perceptuales y semánticas (Roediger & McDermott, 1993; Weldon, 1991). Citado por (Razumiejczyk, López Alonso, & Macbeth, 2008).

Digital Library, 2018, pág. 21). Otros dos de los mejores analistas en contraterrorismo en redes sociales también notaron aquellos esquemas similares en torno a las discusiones de los *trolls* sobre Siria, Assad, al Qaeda y el Estado Islámico (Weisburd, Watts , & Berger, 2016). Las cuentas *Hecklers*, sincronizadas con cuentas de seguimiento, entonces atacaron objetivos políticos usando temas de conversación y patrones de rastreo similares. Las identidades previamente fueron fichadas y simultáneamente aparecieron en diferentes comunidades y locaciones geográficas debido al rastreo de hashtags tales como #Nuclear, #Media, #Trump y #Benghazi, cuyos posts fueron explayados por el empuje de otras cuentas automatizadas. Así mismo hallaron en perfiles de usuario de Twitter de habla inglesa palabras claves como Dios, Militar, Trump, Familia, País, Conservador, Cristiano, América y Constitución. De manera que estos perfiles digitales configuraron en el entorno virtual el nivel intencional de desinformación dado el "objetivo claro de engañar por parte de los promotores y realizadores de la información" (Rodríguez Andrés, 2018, pág. 235) y a la vez, generaron manipulación episódica por cuanto "…la comprensión no consiste solo en la asociación de significados y palabras, oraciones o discursos, sino en la construcción de modelos mentales en la memoria episódica, que incluyen nuestras propias opiniones y emociones asociadas con un evento oído o leído" (van Dijk, 2006, pág. 54).

Muy cerca a la anterior estrategia se halló un segundo perfil para manipular la comprensión del discurso. Fueron cuentas digitales *Honeypots* [se usan en la seguridad informática para atraer y analizar ataques de *bots* o de hacker] que parecían ser "jóvenes mujeres atractivas y apasionadas por entablar amistad con ciertos miembros de los partidarios políticos, a través de la ingeniería social" (Weisburd, Watts , & Berger, 2016, pág. 22). Este segundo proceso estratégico inmediato "opera a distintos niveles de la estructura del discurso, siendo hipotético: se hacen conjeturas rápidas y eficientes y se toman atajos en lugar de hacer análisis completos" (van Dijk, 2006, pág. 53). Un tercer perfil de cuentas digitales pro-Rusia detectado fueron los *bots* automatizados, cuyas violaciones a la denegación de datos penetraron el portal web de la Casa Blanca para alojar el mensaje "Alaska Back To Russia". Fue una campaña pública para devolver el estado más grande de Estados Unidos a la nación que la vendió. El plan obedeció a

generar la tercera clase de manipulación -de la cognición social- ya que "…la forma más influyente de manipulación… se centra en… conocimientos abstractos más generales, como saberes, actitudes e ideologías" (van Dijk T. , 2006, pág. 56).

Tres años antes a las declaraciones de Watts, corporaciones de ciberseguridad privada y agencias nacionales de inteligencia norteamericanas enfocaron su rastreo a los ataques informáticos del grupo "Shaltay Boltai" (en ruso "*Humpty Dumpty*"), un equipo hacker con sede en Rusia y blog en Internet, que a menudo se denominada APT28 o "Fancy Bear". Con un nivel de confianza medio, la empresa de seguridad cibernética Crowd Strike ha mencionado que APT28 está asociado con la agencia de inteligencia militar rusa GRU para apoyar su operación de inteligencia utilizando malware desde al menos el año 2007 (FireEye iSight Intelligence, 2017). Según Kevin Mandia, ex Oficial de Seguridad Informática del Pentágono y CEO de FireEye, "APT28 comprometió a alguna organización como víctima al robarle información mediante operaciones conducidas por falsos hacktivistas, incluyendo, entre otros, perfiles digitales como 'CyberCaliphate', 'CyberBerkut', 'Guccifer 2.0', 'DC Leaks', 'Anonymous Poland'" (Homeland Security Digital Library, 2018, pág. 32).

Este plan de desinformación como arma de ataque contra el adversario traspasa el engaño o el suministro de información falsa y se dirige a deslegitimar al rival en el marco de las relaciones internacionales o en las disputas regionales y, conforme el nuevo orden mundial, ha ido cambiando hacia la multipolaridad con la aparición de nuevos actores internacionales y nuevos conflictos.

> Lo que busca en el fondo esta desinformación es aniquilar a su presunto adversario con base en la palabra y en la trampa psicológica destinadas a obtener la victoria sin combatir dentro de las rivalidades internacionales a fin de crear confusión en el enemigo, desprestigiar a una personalidad pública, manipular a la opinión pública, presionar a los organismos internacionales… (Rodríguez Andrés, 2018, pág. 239).

La superficie del iceberg muestra evidencias del regreso de Rusia a la escena mundial a través de la desinformación (*dezinformatsia*) y el empleo de técnicas de manipulación tanto abiertas como encubiertas (*kombinatzia*) en el entorno virtual que gestionan perfiles digitales –humanos y ciborg-, creados mediante el extraordinario desarrollo de la inteligencia artificial que logra amplia capacidad de programación automática y gran autonomía de decisión sobre los contenidos y los tonos de las discusiones. “Estas "personas" se apropiaron de hacktivistas o de marcas políticas preexistentes con las que pueden ofuscar su verdadera identidad, proporcionar una negación plausible y crear la percepción de credibilidad” (Homeland Security Digital Library, 2018, pág. 32). Subyace empero todavía una crisis de legitimidad y de credibilidad social cuya causa investigada se relaciona con las redes sociales que movilizan personas, corrigen abusos de poder, denuncian, y traslapan acciones deliberadas, organizadas, persistentes, sistemáticas, que manipulan, fabrican información, desarrollan agravios, atiborran insultos, etc.

> Si hace años las redes sociales eran instrumento de participación, de difusión de información que no pasaba por los medios de comunicación –controlados por los gobiernos o por las corporaciones capitalistas-, de libertad no controlada por los poderes políticos, económicos, financieros, actualmente esos mismos poderes y otros de todo tipo, han desplazado la construcción de discursos y de representación a las redes (Castells, 2018).

Los modos de atacar

Mencioné en la introducción que cuatro nuevas palabras rusas hubieron de apropiar tanto la academia como las agencias de inteligencia norteamericanas debido a las operaciones de influencia de Rusia al momento de la elección presidencial en Estados Unidos del año 2016. Analizo en adelante las faltantes -medidas activas (*aktivniye meropriyatiya*) y material comprometedor (*kompromat*)- como modos estratégicos de atacar utilizando en la comunicación agentes involuntarios.

Thomas Rid argumentó ante el SSCI que "…es imposible comprender las operaciones cibernéticas del siglo 21 sin entender primero las operaciones de inteligencia del siglo 20" (U.S. Senate Select Committee on Intelligence, 2018, pág. 41), que provenían del régimen Soviético de preguerra. Richard Shultz y Roy Godson definieron las medidas activas como:

> ciertas técnicas encubiertas, de naturaleza política principalmente, a través del engaño y la distorsión de la percepción de la realidad para influenciar objetivos (elite de gobierno, instituciones no gubernamentales, audiencias masivas, personas extranjeras o nacionales) con base en eventos y comportamientos en la acción llevada a cabo en países extranjeros y que influirán en las políticas de otro gobierno, socavando la confianza de sus líderes e instituciones, perturbando las relaciones entre otras naciones, y desacreditando y debilitando a los gobiernos y opositores no gubernamentales (Shultz & Godson, 1984).

Desde el lado de la inteligencia soviética, Oleg Kalugin, Mayor General en retiro y ex miembro del Comité de Seguridad del Estado Soviético, la describía como:

> …el corazón y el alma de la inteligencia soviética. No es recopilación de inteligencia sino subversión, mediante medidas activas, para debilitar a Occidente, para impulsar presiones de todo tipo en las alianzas de la comunidad occidental -en particular la OTAN-, para sembrar la discordia entre los aliados, para debilitar a Estados Unidos ante la gente de Europa, Asia, África, América Latina, y así preparar el terreno en caso de que realmente ocurra la guerra. Hacer que Estados Unidos sea más vulnerable a la ira y la desconfianza de otros pueblos (CNN, 2007).

Ya se trate de técnicas políticas encubiertas o de subversión, actividades estas orientadas a lograr como objetivo influir en sentido negativo o en la debilidad de extranjeros, las medidas activas pueden ser clasificadas desde la academia como falta de verdad informativa. Esta subclase de desinformación ejecutada, en el caso que analizo, agrupó los tres niveles diferenciados por Durandin: supresión (hacer pensar que lo que existe, no prexiste), adición (hacer admitir lo que en verdad no es evidencia) y deformación (hacer

alterar la naturaleza de las cosas) (Durandin, 1995). Otros académicos más especializados en el estudio de la desinformación como disciplina comunicativa aseguran que es la "comunicación que intencionalmente contiene información falsa, incompleta o engañosa (…) transmitida con el fin de engañar, dar información incorrecta o inducir al error" (Shultz & Godson, 1984, pág. 38). Citado en Rodríguez Andrés (Rodríguez Andrés, 2018, págs. 236-237), Watzlawick habla de la desinformación como operación para engañar y desorientar a adversarios; Benesch & Schmandt la describen como información falsa; Jacquard, como sutil deformación de la verdad; Barron, como diseminación de información falsa y provocadora; Cathala, como método para travestir o disimular la realidad; Galdón, como ausencia de verdadera información o de información verdadera y Fraguas de Pablo sostiene que la desinformación tiene la intención de disminuir, suprimir o imposibilitar la correlación entre la representación del receptor y la realidad del original. De modo tal que la desinformación como falta de verdad se configura en la actual actividad política mediática, conformando a su vez la segunda causa de la crisis de legitimidad y de credibilidad estudiada por la sociología. La política del escándalo conduce a la personalización de la política y esta lleva a prácticas informacionales mezcladas de verdad, media verdad y manipulación. Es decir,

> …el proceso político se ha caracterizado desde hace mucho tiempo como política mediática -única política sobre las cosas que existen siempre y cuando existan primero en los medios de comunicación- y política informacional, capacidad de hacer llegar información moderada o de opinión a través de grandes sistemas de datos lo que permite predecir posibles comportamientos electorales de ciertos sectores y territorios, y en consecuencia dirigir ciertos mensajes pre-fabricados para esos sectores de población (Castells, 2018).

Las modalidades estratégicas

Un examen a los modos de ejecución de las medidas activas rusas del año 2016 comprueba la explotación de las debilidades existentes en la política de Estados Unidos

con el propósito de transferir presiones preexistentes del adversario contra sí mismo. Esta causa de la causa genera una consecuencia de la consecuencia: "cuanto más polarizada está una sociedad más vulnerable es y… las medidas activas son operaciones de inteligencia semi-encubiertas o encubiertas para moldear decisiones políticas del adversario" (Homeland Security Digital Library, 2018, pág. 41).

Los especialistas en inteligencia aseguran de manera general que los transgresores casi siempre ocultan o falsifican la fuente de información porque tratan de esconderse detrás del anonimato o de falsos símbolos para propagar el contenido totalmente falseado o parcialmente adulterado. Con la evidencia pública disponible se comprende ahora que las medidas activas ejecutadas por las agencias de inteligencia de Rusia contra la campaña presidencial norteamericana del 2016 fueron extraordinariamente fuertes al reutilizar elementos en tres circunstancias principales, lo que a su paso generó el uso de material comprometedor (*kompromat*):

a) Implantes: softwares *malware* que habían sido desplegados en gran cantidad durante la última década para intrusiones rusas en docenas de países. Fueron vueltos a usar por los ilegales en las filtraciones al servidor de correos electrónicos del DNC. Esos implantes comparten características comunes como si fueran dispositivos de escucha: un protocolo de comunicación específico y una función modular que aplica exactamente el mismo malware en diferentes servidores sin revelar jamás el diseño.

b) Infraestructura de comando y control: un software reciclado por las agencias rusas de inteligencia que abre las puertas a otro programa informático que contamina las computadoras. Es semejante a disponer el mismo automóvil para escape con una única licencia idéntica para múltiples casos de robo. Esta infraestructura de comando y control difícil de fingir permitió a los investigadores vincular con alta confianza la violación del DNC del año 2016 a otras situaciones previas como el primer hackeo al Bundestag en el año 2015, que el gobierno de Ángela Merkel ya había atribuido a la inteligencia militar rusa GRU.

c) Claves de cifrado: envolturas de algoritmo de criptografía que los operadores rusos también reutilizaron en la escritura de documentos remitidos a diferentes destinos. Los

primeros indicios señalan como víctima a las unidades de artillería de Ucrania desplegadas contra los separatistas que apoyaba Rusia. Esta superposición criptográfica es un enlace excepcionalmente fuerte comparable a una huella digital humana.

Los agentes involuntarios

La inteligencia técnica ha sido explotada por las agencias rusas de inteligencia por cuanto los gadget son perfectas barreras para el anonimato, la piratearía y el robo de información. Para la campaña presidencial entre Hillary Clinton y Donald Trump, el profesor Rid destaca tres tipos diferentes de agentes involuntarios comprometidos, a saber:

a) Wikileaks red creada para ocultar robos de información convertida en discutida organización mediática internacional sin ánimo de lucro que apoya la libertad de expresión a través de la publicación de informes anónimos y documentos filtrados con contenido sensible en materia de interés público. Fue ideal para los operadores de las medidas activas, en especial oficiales rusos de inteligencia. Probablemente se encargaron de utilizar la red como su antiguo libro de jugadas soviéticas: "…cualquier agente involuntario en terreno es más efectivo cuando se le hace creer que realmente está favoreciendo una íntegra moral, porque no representa a una agencia de inteligencia autoritaria" (Homeland Security Digital Library, 2018, pág. 45).

b) Twitter siendo la plataforma de red social más influyente entre los líderes de opinión, prácticamente es la perfecta para perpetrar medidas activas debido a su fácil explotación con alto impacto. Bots totalmente automatizados, así como cuentas semiautomáticas de correo no deseado y trolling constituyen una parte considerable de la base de usuarios activos. Con esos bots automatizados o semiautomatizados amplificaron la desinformación o intimidaron a los oponentes. No obstante, se desconoce cuántas interacciones y compromisos eran cuentas humanas políticamente influyentes durante la campaña del 2016 ni cuántos de esos compromisos fueron controlados desde el extranjero o deliberadamente engañosos.

c) Periodistas, el tercer grupo de agentes involuntarios quienes cubrieron ofensivamente las filtraciones políticas de 2016 pero también descuidaron o ignoraron la procedencia de las fuentes de información. “Las medidas activas del bloque soviético en muchos cientos de veces alimentaron hábilmente falsificaciones y documentos seleccionados para periodistas” (Homeland Security Digital Library, 2018, pág. 46). Ocasionar tal trabajo requirió de mano de obra y artesanía mediante acciones como: preparación de documentos, redacción de cartas de presentación, diseño de portadas para informes encubiertos, construcción de confianza y ejecución de operaciones complejas de desinformación. Fueron los mismos periodistas estadounidenses quienes cayeron víctimas y cavaron profundamente grandes vertederos produciendo joyas informativas o realizando minería de noticias, sin saber que impulsaban las operaciones.

Integrando comprendo que la innovación en las inteligencias técnica y humana soviéticas apaleó al salto cuantitativo y cualitativo hacia las inteligencias técnica y humana rusas gestionando desinformación organizada operada desde una ingeniería social. La característica reciente reside en la sistematicidad con que se llevó a cabo y en la dotación de cierto carácter de profesional que imprimió - ¿o sigue? - poder desde instituciones, organismos, departamentos específicos, etc. La Oficina del Director Nacional de Inteligencia (ODNI) de Estados Unidos ha dejado claro que en el año 2008 los servicios de inteligencia del extranjero señalaron a las campañas electorales como objetivos críticos. Los agentes aprovecharon reuniones con contactos personales y de campaña, uso de redes humanas para compartir ideas políticas, explotación de la tecnología para obtener datos sensibles y comprometer pagos por la gestión de influencia en la percepción política (Oficina del Director Nacional de Inteligencia, 2016). Kalugin sostiene que la inteligencia humana “…proporcionó la mayor parte de la información requerida por el gobierno de Rusia a través de actividades de comercio o robos como el ejecutado a IBM” (CNN, 2007).

Dicha ingeniería social supero al conjunto de técnicas que usan los cibercriminales para crear vulnerabilidades de software con base en versiones de emociones humanas para que los ataques sean exitosos y se engañe a los incautos usuarios con envío de datos confidenciales, infección de computadoras o enlaces a sitios web envenenados. A nivel de

globalización y de procesos de identificación, la crisis de legitimidad y de credibilidad presenta un desfase entre los espacios de lo global y lo local en donde las instituciones sostenidas por los ciudadanos "no responden a su compromiso de protección de la vida y ponen en cuestión su representatividad" (Castells, 2017, pág. 78). La desconfianza ciudadana por las instituciones, ocasionada en los procesos de identificación, "atrinchera" a las identidades con lo que se reafirma la comunidad nacional con respecto a lo que es el estado nación. Adicional, en los sistemas políticos se expresa la corrupción sistémica definida como "toma de decisiones intencionales -políticas y administrativas- de responsables políticos en beneficio de intereses privados a cambio de dinero o servicios a favor de los garantes públicos" (Castells, 2018). Las causas del menoscabo en la representatividad institucional se hallan en la cierta independencia de los *mass media* frente a la comunicación de masas mientras que las de la corrupción en los sistemas políticos se explican desde los individuos quienes gestionan en red para obtener el máximo beneficio posible sin intermediación. No obstante, las causas primeras obedecerían al hundimiento de las ideologías y a las prácticas de recompensa de los individuos que ingresan a lo público (léase, lo político) circunscritas por los datos y por los sistemas de información que controlan el mal hacer de aquellas.

Finalmente, la desinformación organizada planeada a través de las inteligencias técnica y humana rusas y gestionada desde una ingeniería social es otro minucioso modo de manipulación constituido, estructurado, proyectado, que responde tanto a estrategias concretas como a fines políticos inteligibles. Vinculada en este caso de análisis a las relaciones internacionales, lo más común que se determina es la fuente de los procedimientos que recae en los estados a través de sus aparatos de inteligencia y ya no de propaganda como las sucedidas cuando se estableció el Ministerio del Reich alemán para la ilustración pública y de propaganda. El receptor es igualmente otro estado considerado como adversario. Esta planificación "…es una comunicación no atribuible a fuentes falsas" (Shultz & Godson, 1984, pág. 38) y cuyas instituciones responsables por la desinformación organizada dejaron de lado cualquier consideración ética en el cumplimiento de sus propósitos, persiguiendo solo efectividad y éxito en sus misiones.

Algunos de los quince miembros del SSCI, en la sesión del 30 de marzo de 2017, se preguntaron ¿por qué el gobierno de Rusia está involucrado en esta gran escala diversificada de operaciones de influencia? El testigo Godson reaccionó por estas técnicas de influencia observando la mentalidad de generaciones de los líderes rusos que "proporcionan una ventaja estratégica y táctica en sus instituciones políticas para afectar los resultados políticos significativos en el extranjero. Ellos lo dicen. Ellos lo hacen. Pero no en los altos niveles" (Shultz & Godson, 1984, pág. 10). Rumer también se inclinó en que existen ventajas importantes para Rusia, dado que "no hay audiencia doméstica ante la cual el gobierno rinda cuenta de sus acciones en el exterior, pues el Kremlin tiene poca o ninguna restricción externa en el mecanismo simplificado de toma de decisiones" (Homeland Security Digital Library, 2018, pág. 8). Mandia confirmó que "…los objetivos geopolíticos de Rusia han hecho evaluar a nuestra confianza, que ha crecido, con respecto a que el gobierno ruso patrocina un espionaje de largo plazo con muchos recursos" (Homeland Security Digital Library, 2018, pág. 35). Watts respondió que "Rusia busca ganar la segunda guerra fría a través de… Internet y las redes sociales como puertas de acceso para llegar hasta las audiencias extranjeras, baratas, eficientes y altamente efectivas... creando divisiones políticas en la Unión Europea y la OTAN" (Homeland Security Digital Library, 2018, pág. 25).

Conclusiones

1- Con base en perspectivas académicas, si la comprensión de un discurso manipulativo en sentido semiótico que incide en la memoria de largo y corto plazo puede ser ejercido mediante procesamiento de información, conocimiento, actitudes e ideologías distribuidas dentro de un contexto social, la guerra de desinformación ejecutada en Estados Unidos para la elección presidencial del presidente 45 se configuró en la pragmática de la cognición social igualmente manipulada a través de estrategias militares rusas de dos tipos: medidas activas y campañas de influencia (sobre mensajes engañosos, propaganda falsa, agentes involuntarios). Ambas provienen de la defensa Bolchevique, grupo político radicalizado dentro del Partido Obrero Socialdemócrata de Rusia -dirigido

desde un principio por Vladímir Ilich Uliánov (Vladímir Lenin) y posteriormente por Iósif Vissariónovich Dzhugashvili (Joseph Stalin)-, que Rusia volvió a retomar en cabeza de Vladímir Vladímirovich Putin para ejecutar una amplia campaña de desinformación intencional como arma de ataque no letal contra su adversario.

2- Una práctica de los efectos estudiada en el marco de la comunicación política encierra ciertas condiciones sociales para hacer efectivo aquel control con base en la formulación de discursos expresados en términos de pertenencia del grupo, de la posición institucional, de la profesión, de los recursos materiales o simbólicos. Por tanto, la desinformación en aquel año 2016 en Estados Unidos ejecutada mediante acciones de grupos hacker, medios de comunicación, redes sociales –Wikileaks y Twitter-, periodistas quienes cubrieron ofensivamente las filtraciones políticas, ciudadanía, agentes sociales, se elevó a menoscabo de la verdad en los mensajes y que ligado a la información y al contenido de los mass media clasifica la ejecución como acontecimiento organizado por un régimen menospreciado por el utilitarismo globalizado. El resultado de hacer tamaña ingeniería social adoptando medidas activas en el entorno digital no solo reduce costos de operación, sino que, según la empresa consultora estadounidense Media Quant, Donald Trump gastó 10 millones de dólares en anuncios y consiguió gratis una cobertura que a otro candidato le hubiera costado 2.500 millones de dólares (Restrepo, 2016).

3- Las medidas activas soviéticas para los momentos de la Guerra Fría tenían como objetivo principal “desacreditar, debilitar a los oponentes y distorsionar la percepción de la realidad”. Con las implementas por los equipos rusos, la defensa se eleva a la Guerra de Nueva Generación (NGW): estrategia de influencia que excluye la fuerza bruta y se ajusta al entorno virtual redistribuido desde agentes involuntarios, enigmáticos entusiastas acosadores, falsas identidades virtuales, bots automatizados que igualmente aprovechan los conflictos internos de una sociedad polarizada por la crisis de legitimidad y de credibilidad.

REFERENCIAS BIBLIOGRÁFICAS

Abelino, H. (2017). *Las leyes de la Comunicología.* Quito: Editorial Razón y Palabra.

Alexander, K. (22 de March de 2017). *A Borderless Battle: Defending Against Cyber Threats.* Recuperado el 30 de junio de 2017, de U.S. House of Representatives: docs.house.gov/meetings/HM/HM00/20170322/105741/HHRG-115-HM00-Wstate-AlexanderK-20170322.pdf

Arribas, F., & Barberá, R. (2018). La Revolución Bolchevique: los origenes de la propaganda y la manipulación de la opinión pública. *Historia y comunicación social*, 23(1), 49-63.

Castells, M. (1996). *La era de la información: economía, sociedad y cultura, Volumen I.* Madrid: Alianza Editorial.

Castells, M. (2017). *Ruptura: la crisis de la democracia liberal.* Madrid: Alianza Editorial.

Castells, M. (12 de diciembre de 2018). *La crisis global de la democracía liberal*. Recuperado el 15 de enero de 2019, de ORAIN GIPUZKOA: https://youtu.be/1iAIqS4lpHs

Cathala, H. (1986). *Le temps de la désinformation.* Paris: Stock.

Clapper, J. (26 de February de 2015). *Opening Statement to Worldwide Threat Assessment Hearing.* Recuperado el 10 de junio de 2018, de ODNI: https://www.dni.gov/files/documents/2015%20WWTA%20As%20Delivered%20DNI%20Oral%20Statement.pdf

CNN. (6 de February de 2007). *Inside the KGB. An interview with retired KGB Maj. Gen. Oleg Kalugin.* Recuperado el 8 de junio de 2018, de CNN Interactive: https://web.archive.org/web/20070206020316/http:/www.cnn.com/SPECIALS/cold.war/episodes/21/interviews/kalugin/

Durandin, G. (1995). *La información, la desinformación y la realidad.* Barcelona: Paidós.

Eveland, W. (2003). A 'mix of attributes' approach to the study of media effects and new communication technologies. *Journal of Communication*, 53 (3), 395-410.

FireEye iSight Intelligence. (January de 2017). *APT28: At the center of the storm. Russia Strategically Evolves its Cyber Operations.* Recuperado el 29 de junio de 2018, de Fire Eye: https://www2.fireeye.com/rs/848-DID-242/images/APT28-Center-of-Storm-2017.pdf

García-Avilés, J. (2009). La Desinformación. En J. Herrero, *Manual de Teoría de* (págs. 332-350). Madrid: Universitas.

Homeland Security Digital Library. (30 de March de 2018). *Disinformation: A Primer in Russian Active Measures and Influence Campaigns.* Obtenido de HSDL: https://www.hsdl.org/?view&did=802222

Jacquard, R. (1988). *La desinformación: una manipulación del poder.* Madrid: Espasa.

MacFarquhar, N. (28 de Agosto de 2016). A Powerful Russian Weapon: The Spread of False Stories. *New York Times*, págs. https://www.nytimes.com/2016/08/29/world/europe/russia-sweden-disinformation.html.

McQuail, D. (2000). *Introducción a la teoría de la comunicación de masas.* Barcelona: Paidós.

Milosevich-Juaristi, M. (2017). *El poder de la influencia rusa: la desinformación.* Real Instituto Elcano: Madrid.

Oficina del Director Nacional de Inteligencia. (4 de November de 2016). *Unlocking the Secrets: How to Use the Intelligence Community.* Recuperado el 4 de junio de 2018, de ODNI: https://www.dni.gov/files/documents/FOIA/DF-2015-00025.pdf

Reasonwhy. (26 de enero de 2018). *¿Cómo enseñan a contrastar las fuentes en la era de Internet?* Recuperado el 16 de noviembre de 2019, de Reasonwhy: https://www.reasonwhy.es/reportaje/como-ensenan-contrastar-las-fuentes-en-la-era-de-internet

Restrepo, J. (4 de noviembre de 2016). *Informar en épocas electorales ¿Tienen responsabilidad los medios en la fama desbordada de Trump?* Recuperado el 15 de noviembre de 2019, de Fundación Gabo: https://fundaciongabo.org/es/consultorio-etico/consulta/1563

Rodríguez Andrés, R. (2018). Fundamentos del concepto de desinformación como práctica manipuladora en la comunicación política y las relaciones internacionales. *Historia y comunicación social*, 23(1), 231-244.

Romero-Rodriguez, L. (2014). *Pragmática de la desinformación: Estratagemas e incidencia de la calidad informativa de los medios.* Huelva (España): Universidad de Huelva.

Shultz, R., & Godson, R. (1984). *Dezinformatsia: active measures in Soviet strategy.* Washington: Pergamon-Brassey's.

Sokolovsky, V. (1981). *Estrategia militar soviética.* Madrid: Ediciones Ejército.

U.S. Senate Select Committee on Intelligence. (8 de May de 2018). *Russian Targeting of Election Infrastructure During the 2016 Election: Summary of Initial Findings and Recommendations.* Recuperado el 29 de junio de 2018, de Publications: https://www.intelligence.senate.gov/publications/russia-inquiry

van Dijk, T. (1984). *Texto y contexto: semántica y pragmática del discurso.* Madrid: Cátedra.

van Dijk, T. (1996). Discourse, power and access. En C. Caldas-Coulthard, & M. Coulthard, *Texts and practices: Readings in critical discourse analysis* (págs. 84-104). London: Routledge.

van Dijk, T. (2006). Discurso y manipulación: Discusión teórica y algunas aplicaciones. *Signos*, 39(60), 49-74.

Vosoughi, S., Roy, D., & Aral, S. (2018). The spread of true and false news online. *Science Review*, 359 (6380), 1146-1151.

Weisburd, A., Watts , C., & Berger, J. (6 de November de 2016). *Trolling for Trump: How Russia Is Trying to Destroy Our Democracy.* Recuperado el 15 de junio de 2018, de War on the rocks: https://warontherocks.com/2016/11/trolling-for-trump-how-russia-is-trying-to-destroy-our-democracy/