INSTITUTO DE CIBERDEFENSA DE LAS FUERZAS ARMADAS

DIPLOMATURA UNIVERSITARIA EN GESTIÓN DE LA CIBERDEFENSA

TRABAJO FINAL INTEGRADOR

ANÁLISIS DE LAS OPERACIONES DE INFLUENCIA EN EL CIBERESPACIO: CASOS DE ESTUDIO Y TENDENCIAS EMERGENTES.

INTEGRANTES DEL GRUPO NRO 7:
MAXIMILIANO AZCURRA
DARÍO FERNANDO CARO
WALTER BENITO MINCHACA
DIEGO DELGADO RIVEROS

Títulos Profesionales / de grado

Licenciado en Administración- Magister en Educación
Ingeniero en Computación
Ingeniero en Telecomunicaciones
Abogado - Licenciado en Criminalística

04 de Noviembre de 2024

Resumen

Este trabajo tiene como objetivo general analizar las operaciones de influencia y el ciberespacio a la luz de las nuevas tendencias actuales. Para ello, luego de definir conceptos claves, describimos dos casos actuales donde vemos la interacción de las operaciones de influencia, las operaciones de información y el ciberespacio en las elecciones presidenciales de 2016 en Estados Unidos de América y el Brexit en Europa.

El método a emplear para desarrollar el trabajo de investigación será del tipo deductivo, con ciertas inferencias inductivas, para ello se realizarán distintos análisis y descripciones durante el desarrollo de cada capítulo a fin de obtener conclusiones parciales surgidas de cada uno de ellos y que permitan dar respuesta al objetivo general planteado por la investigación.

Concluimos que las operaciones de influencia tienen gran un impacto social, económico y político para los Estados y para las personas donde el ciberespacio cumple un papel fundamental.

Reflexionamos que poner en marcha acciones de educación digital, transparencia de las plataformas, verificación de hechos y cooperación internacional son las claves para lograrlo.

Palabras Claves: ciberespacio, operaciones de influencia, tendencias emergentes.

Índice General

Resumen 1
Indice General……2
INTRODUCCIÓN 3
LAS OPERACIONES DE INFLUENCIA EN EL CIBERESPACIO 4
Definición de Operaciones de Influencia en el ciberespacio. 4
Características de las Operaciones de Influencia 4
Objetivos Comunes 5
Impacto y Consecuencias 6
Defensas y Mitigación 6
Marco Teórico 7
Historia de la propaganda y la manipulación de la información. 7
Orígenes y evolución 7
Tipos de Operaciones de Influencia: 7
Referencia de las Operaciones de Influencia en el Manual de Tallin. 8
Operaciones de Influencia vs. Operaciones de Información – Comparativa 8
Similitudes 8
Diferencias 9
Interrelación 9
CASO 1: Interferencia rusa en las elecciones presidenciales de EEUU de 2016……..…10
CASO 2: BREXIT……13
Tendencias Emergentes……18
Conclusión 21
Referencias……...23

INTRODUCCIÓN

En este trabajo se analizan las operaciones de influencia y el ciberespacio, algunos casos emblemáticos para entender más la problemática, además de tendencias emergentes. En efecto, se recogen algunas de las prácticas "manipuladoras" que se ha observado desde diferentes ámbitos como la publicidad y el marketing, e intentaremos deducir, entre otras cosas, lo fácil que resulta utilizar estas prácticas para aquellos grupos que deseen comunicar mensajes al margen del respeto a la veracidad y al rigor de la información.

De esta manera, estamos frente a un escenario de una guerra de información, que como advierte Rianne Van Vuuren (2015), citado en Ventre (2016), son aquellas "acciones centradas en desestabilizar o manipular las redes de información centrales de un estado o entidades en la sociedad con el objetivo de influir en la capacidad y la voluntad de proyectar poder, así como los esfuerzos para contrarrestar ataques similares de una entidad y/o estado opuesto" (p. 273).

Es en este momento cuando se comienza a estudiar las posibles influencias que los mensajes personalizados o hiperpersonalizados del *microtargeting*[1] ejercen en los ciudadanos. Asimismo, a lo largo del presente trabajo puede evidenciarse las dificultades para identificar las iniciativas de microtargeting o hiperpersonalización y los riesgos derivados de la opacidad con relación a la misma. (García, 2023)

En efecto, el ciberespacio entendido como un ámbito en donde la "traducción del conflicto desde el mundo real a uno virtual introduce nuevos aspectos en la disputa" es signado claramente por dos características: la asimetría y la velocidad. Al respecto, Ventre (2016) afirma:

> Las operaciones de información pueden ser ofensivas y defensivas. Las operaciones de información ofensivas son el uso integrado de métodos y actividades específicas, apoyados por la inteligencia, para afectar a los tomadores de decisión enemigos o influir en otros. El efecto deseado es destruir, deteriorar, interrumpir, engañar, explotar e influir en las funciones enemigas. Los objetivos finales son los líderes y los procesos de decisión humana del adversario o de terceros que se encuentren en la zona de operaciones (p.44)

En línea con el hecho de estar frente a un espacio en el que valen reglas distintas y la disputa adquiere una velocidad tal que no hay tiempo para la toma de decisiones reflexivas,

[1] El microtargeting es una forma de publicidad dirigida en línea que analiza datos personales para identificar los intereses de una audiencia o individuo específico con el fin de influir en sus acciones, ofreciendo un mensaje personalizado a una persona o audiencia mediante un servicio en línea como las redes sociales.

uno de los mayores problemas radica en que los incidentes se presentan con dos características claves: acotan entre sí el conflicto y los ciberataques manifiestan un nivel de agresión que bien puede ser utilizado como presagio de un ataque militar real. (Moresi et al., 2023)

LAS OPERACIONES DE INFLUENCIA EN EL CIBERESPACIO

Definición de Operaciones de Influencia en el ciberespacio.

Las operaciones de influencia en el ciberespacio son acciones estratégicas y deliberadas diseñadas para manipular la opinión pública, las percepciones y los comportamientos de individuos o grupos a través de medios digitales. Estas operaciones, a menudo encubiertas, buscan alcanzar objetivos específicos, como influir en procesos políticos, económicos o sociales, y pueden ser llevadas a cabo por gobiernos, organizaciones, grupos o incluso individuos.

Características de las Operaciones de Influencia

1. **Intencionalidad:** Decimos que las Operaciones de Influencia tienen intencionalidad ya que se llevan a cabo a través de acciones planificadas y con un propósito definido.

   La intencionalidad es un elemento fundamental en cualquier operación de influencia, ya sea en el mundo físico o en el ciberespacio. En el contexto digital, esta cualidad adquiere una particular relevancia debido a la capacidad de manipular la información y las percepciones a gran escala y con una rapidez sin precedentes.

2. **Manipulación:** Buscan influir en las creencias, actitudes y comportamientos de las personas de manera no transparente. La manipulación es un elemento central en estas operaciones, y se lleva a cabo a través de una variedad de tácticas y técnicas como lo son:

   a. **Desinformación:** La creación y difusión de información falsa o engañosa es la táctica más común. Esto puede incluir:

      1) **Noticias falsas:** Artículos o publicaciones que presentan información completamente fabricada como si fueran hechos reales.

      2) **Contenido fabricado:** Imágenes, videos o audios manipulados para crear una narrativa falsa.

3) **Citas falsas:** Atribuir a personas o instituciones declaraciones que nunca hicieron.

b. **Descontextualización:** Sacar fragmentos de información de su contexto original para darle un significado completamente diferente.

c. **Polarización:** Exagerar las diferencias entre grupos sociales o políticos para fomentar la división y el conflicto.

d. **Bots y cuentas falsas:** Utilizar software automatizado y perfiles falsos para amplificar mensajes y simular un mayor apoyo a una determinada idea.

e. **Técnicas de persuasión:** Aplicar principios psicológicos para influir en las emociones y creencias de las personas, como el miedo, la ira o la esperanza.

¿Por qué es tan efectiva la manipulación en el ciberespacio?

Esto es posible debido a las características propias que brinda el ciberespacio, como lo es:

1. **Velocidad de difusión:** La información falsa se puede propagar rápidamente a través de las redes sociales y otros canales digitales.
2. **Alcance global:** Las operaciones de influencia pueden llegar a audiencias masivas en todo el mundo.
3. **Anonimato:** Los actores que llevan a cabo estas operaciones pueden ocultar su identidad, lo que dificulta la atribución de los hechos a los autores.
4. **Dificultad de verificación:** Verificar la autenticidad de la información en línea puede ser difícil y requiere tiempo.
5. **Algoritmos de las redes sociales:** Los algoritmos de las plataformas sociales pueden amplificar contenido polarizador y engañoso.

Objetivos Comunes

Entre los objetivos más comunes que suelen perseguir las operaciones de Influencia en el Ciberespacio podemos mencionar a los que buscan:

1. **Influir en elecciones:** Aquí lo que se busca es alterar el resultado de procesos electorales mediante la difusión de información falsa o la manipulación de la opinión pública.
2. **Desestabilizar gobiernos:** Sembrar discordia y desacuerdo en sociedades estables.

3. **Promover agendas políticas:** Impulsar determinadas ideologías o causas.
4. **Dañar la reputación:** Desacreditar a individuos, organizaciones o países.
5. **Obtener ventajas económicas:** Influir en los mercados financieros o en las decisiones de consumo.

Impacto y Consecuencias

1. **Erosión de la confianza:** Mina la confianza en las instituciones y en los medios de comunicación.
2. **Polarización social:** Aumenta las divisiones sociales y dificulta el diálogo.
3. **Interferencia en procesos democráticos:** Amenaza la legitimidad de los sistemas democráticos.
4. **Violencia:** En algunos casos, puede incitar a la violencia y al extremismo.
5. **Desestabilización económica:** Puede afectar negativamente a los mercados financieros y a la economía en general.

Defensas y Mitigación

Las operaciones de influencia en el ciberespacio representan una amenaza creciente para la democracia, la seguridad y la estabilidad de las sociedades. Comprender sus características, objetivos y técnicas es fundamental para desarrollar estrategias efectivas de defensa y mitigación. Los principales tópicos en los que se debe hacer foco son:

1. **Educación digital:** Fomentar el pensamiento crítico y la capacidad de que los individuos sean capaces de evaluar la información.
2. **Verificación de hechos:** Desarrollar herramientas y plataformas para verificar la veracidad de la información.
3. **Transparencia de las plataformas:** Exigir a las plataformas digitales que sean más transparentes sobre sus algoritmos y prácticas.
4. **Cooperación internacional:** Establecer marcos legales y mecanismos de cooperación para combatir las operaciones de influencia.

Marco Teórico

Historia de la propaganda y la manipulación de la información.

La propaganda y la manipulación de la información son prácticas tan antiguas como la comunicación misma. A lo largo de la historia, han sido utilizadas por líderes, gobiernos y organizaciones para influir en las opiniones, creencias y comportamientos de las masas.

Orígenes y evolución

1. Antigüedad: Los primeros ejemplos de propaganda se remontan a la antigua Grecia y Roma, donde los líderes utilizaban oradores y panfletos para movilizar a las masas y ganar apoyo político.
2. Edad Media: La Iglesia Católica empleó la propaganda para difundir sus doctrinas y fortalecer su poder. Los cruzados utilizaron símbolos y canciones para unificar a los creyentes y motivarlos a luchar.
3. Revolución Francesa: La propaganda jugó un papel fundamental en este período, con ambos bandos utilizando panfletos, carteles y canciones para movilizar a la población y justificar sus acciones.
4. Siglo XX: El siglo XX fue testigo de un auge de la propaganda, especialmente durante las guerras mundiales. Tanto los nazis como los aliados utilizaron la propaganda de manera masiva para influir en la opinión pública y ganar apoyo para sus causas.
5. Era digital: Con el advenimiento de internet y las redes sociales, la propaganda ha evolucionado hacia nuevas formas. Las noticias falsas, los bots y las campañas de desinformación se han convertido en herramientas poderosas para manipular la opinión pública.

Tipos de Operaciones de Influencia:

- Operaciones de influencia estatal.
- Operaciones de influencia de actores no estatales (grupos terroristas, empresas, etc.).
- Campañas de desinformación y propaganda.

Referencia de las Operaciones de Influencia en el Manual de Tallin.

En el Manual de Tallin, las operaciones de influencia se mencionan en el contexto de la guerra cibernética, específicamente en la sección sobre "Ataques contra objetos". Se hace una distinción entre las operaciones cibernéticas que tienen como objetivo influir en la moral civil y las que tienen como objetivo destruir o dañar objetos militares.

El Manual establece que las operaciones de influencia dirigidas a la población civil no están prohibidas, siempre y cuando no alcancen el nivel de un ataque. Un ejemplo de una operación de influencia permitida sería la transmisión de mensajes de correo electrónico a la población enemiga exigiendo la rendición.

Sin embargo, el Manual también advierte que las operaciones de influencia dirigidas a objetos militares deben cumplir con los criterios de un objetivo militar legítimo. Esto significa que el objeto debe contribuir de manera efectiva a la acción militar y que su destrucción o neutralización debe ofrecer una clara ventaja militar.

Finalmente, el Manual de Tallin reconoce la existencia de operaciones de influencia en la guerra cibernética, pero establece límites claros para su uso. Las operaciones de influencia dirigidas a la población civil están permitidas, siempre y cuando no alcancen el nivel de un ataque, mientras que las operaciones dirigidas a objetos militares deben cumplir con los criterios de un objetivo militar legítimo.

Operaciones de Influencia vs. Operaciones de Información – Comparativa

Comparativa entre las operaciones de influencia en el ciberespacio y las Operaciones de Información, considerando sus similitudes, diferencias y la interrelación entre ambas.

Similitudes

- **Objetivo:** Tanto las operaciones de influencia como las de información buscan afectar la percepción, el comportamiento y la toma de decisiones de un público objetivo.
- **Dominio de acción:** Ambas operan principalmente en el ciberespacio, aprovechando las tecnologías de la información y la comunicación (TIC) para alcanzar sus objetivos.
- **Técnicas:** Comparten un conjunto de técnicas, como la desinformación, la propaganda, el engaño y la manipulación de la información.

- **Efectos:** Buscan generar efectos psicológicos y cognitivos en el público objetivo, erosionando la confianza, polarizando la opinión pública e interfiriendo en procesos democráticos.

Diferencias

- **Alcance:** Las operaciones de influencia suelen tener un alcance más amplio, buscando moldear el entorno estratégico y la opinión pública en general. Las operaciones de información, en cambio, pueden ser más focalizadas, apuntando a audiencias específicas.

- **Propósito:** Las operaciones de influencia se centran en la manipulación de la percepción y el comportamiento a largo plazo. Las operaciones de información, por otro lado, pueden tener un propósito más inmediato, como obtener información o interrumpir las comunicaciones del adversario.

- **Ética:** Las operaciones de influencia se sitúan en un área gris en términos éticos, ya que pueden implicar la manipulación de la opinión pública y la interferencia en procesos democráticos. Las operaciones de información, si bien también pueden ser utilizadas con fines poco éticos, suelen estar más reguladas y sujetas al derecho internacional.

Interrelación

- **Complementariedad:** Las operaciones de influencia y las de información se complementan mutuamente. Las operaciones de influencia pueden crear un entorno favorable para las operaciones de información, mientras que las operaciones de información pueden ser utilizadas para apoyar y amplificar las operaciones de influencia.

- **Integración:** En muchos casos, las operaciones de influencia y las de información se integran en una estrategia más amplia de ciberseguridad y defensa nacional.

- **Evolución:** Ambas están en constante evolución, adaptándose a las nuevas tecnologías y a las cambiantes dinámicas del ciberespacio.

Luego de definir y clasificar todos los aspectos referidos a las Operaciones de Influencia y el Ciberespacio, es menester desarrollar dos casos donde vemos tomar valor todo lo anteriormente descripto. Estos casos serán presentados a continuación:

CASO 1. Acusaciones de interferencia rusa en las elecciones presidenciales de Estados Unidos de 2016.

Las acusaciones de interferencia rusa en las elecciones presidenciales de Estados Unidos de 2016 se refieren a la conclusión llegada por la Comunidad de Inteligencia de los Estados Unidos, con «gran confianza», de que el gobierno ruso participó en interferencia electoral durante las elecciones presidenciales de Estados Unidos de 2016. De acuerdo con el informe, el presidente de Rusia, Vladímir Putin, ordenó una campaña de influencia en 2016. Las metas del gobierno ruso eran socavar la fe pública en el proceso democrático de Estados Unidos, denigrar a Hillary Clinton y perjudicar su electabilidad y presidencia potencial, afirmando que «evaluamos que Putin y el gobierno ruso desarrollaron una clara preferencia por el presidente electo Trump. Tenemos mucha confianza en estos juicios».

En 2023 el periodista Matt Taibbi, a quien Elon Musk abrió los archivos de Twitter, estableció que la ONG "Alliance for Securing Democracy" fue responsable por miles de reportes noticiosos que falsamente alegaron influencia rusa. Los fundadores de la ONG son asociados de Clinton y de Obama. La Oficina del Director de Inteligencia Nacional (DIN), que representa a 17 agencias de inteligencia y el Departamento de Seguridad Nacional (DSN) declararon conjuntamente que Rusia hackeó el Comité Nacional Demócrata (CND) y filtró sus documentos a WikiLeaks. A principios de enero de 2017, el director de Inteligencia Nacional James Clapper testificó ante un comité del Senado que la supuesta intromisión de Rusia en la campaña presidencial de 2016 fue más allá del hackeo e incluyó desinformación y difusión de noticias falsas a menudo promovidas en las redes sociales. El gobierno ruso negó repetidamente que tuviera alguna participación en los ciberataques al Comité Nacional Demócrata.

Las agencias de inteligencia estadounidenses evaluaron que Putin «dirigió personalmente» la operación. El director de la CIA, John O. Brennan, el director del FBI, James Comey y el DIN James Clapper, coincidieron en «el alcance, la naturaleza y el propósito» de la presunta interferencia de Rusia para ayudar a Trump. Varias empresas de seguridad informática declararon que los ataques cibernéticos fueron cometidos por los grupos

rusos de inteligencia Fancy Bear y Cozy Bear. En octubre de 2016, Obama usó el teléfono rojo para contactar directamente a Putin y emitir una advertencia sobre los ataques cibernéticos.

Obama ordenó un informe sobre las intervenciones extranjeras en las elecciones de 2016. Los senadores estadounidenses pidieron una investigación bipartidista. El entonces presidente electo Donald Trump rechazó inicialmente el informe, diciendo que los demócratas estaban reaccionando a su derrota en la elección, y atacó a las agencias de inteligencia en una declaración de su equipo de transición. El líder de la mayoría en el Senado, el republicano Mitch McConnell, expresó su confianza en la inteligencia estadounidense y apoyó una investigación bipartidista, al igual que el Comité de Inteligencia del Senado. El 29 de diciembre de 2016, Estados Unidos expulsó a 35 diplomáticos rusos, denegó el acceso a dos recintos de propiedad rusa y ampliaron las sanciones existentes a las entidades e individuos rusos.

Tras la invasión rusa de Ucrania, en febrero de 2023, el jefe del Grupo Wagner, Yevgueni Prigozhin, confirmó que creó la Agencia de Investigación de Internet, comúnmente llamada la 'granja de troles', para interferir en las elecciones de EEUU, hecho que estuvo negando durante diez años.

¿Cómo fue el 'hackeo' de piratas informáticos de Rusia durante las elecciones de Estados Unidos?

Según una noticia de la BBC NEWS MUNDO los rusos le dicen "kompromat": usar información política en contra de una persona para dañar su imagen o chantajearla. Material comprometedor es lo que significa esa composición de palabras en ruso y que se usa como táctica en contra de figuras públicas nacionales y extranjeras.

Para las agencias de inteligencia de Estados Unidos, una suerte de "kompromat" es lo que está en investigación. La Agencia Central de Inteligencia (CIA) concluyó que hubo una inferencia ilegal vía ataques cibernéticos en la elección presidencial del 2016.

- ¿El origen? Rusia, presuntamente con un grupo de hackers llamados The Dukes.
- ¿El responsable? El presidente ruso Vladimir Putin, o al menos eso dice el gobierno de EE.UU.
- ¿El objetivo? La campaña presidencial del Partido Demócrata y su candidata, Hillary Clinton.
- ¿El efecto? Un golpe en la campaña de los demócratas.

El email que causó todo

John Podesta era el jefe de la campaña de Hillary Clinton, un antiguo asesor del presidente Barack Obama y parte del equipo de la Casa Blanca. Aquel marzo, cuando estaba en marcha la campaña de las primarias demócratas, Podesta recibió una alerta de correo electrónico. Era una como la que recibe cualquier persona que usa el servicio de Gmail y que dice en letras grandes sobre un fondo rojo "Alguien tiene tu contraseña". Ese correo es el que cualquier usuario del correo de Google recibe cuando ocurre un inicio de sesión sospechoso, desde un lugar inusual o en un dispositivo desconocido.

Para proteger la seguridad de la cuenta, pide que el usuario cambie la contraseña inmediatamente y de esa manera quede bloqueado cualquier nuevo intento de ingreso cuando la clave fue robada. Podesta no hizo clic al instante, sino que envió ese mensaje a su equipo de soporte técnico y ciberseguridad para que se encargaran de comprobar la veracidad de la alerta.

"Este es un correo legítimo", fue el diagnóstico de Charles Delavan, del equipo técnico de Clinton, el 19 de marzo pasado, según una investigación de The New York Times. Hacer clic en el botón "cambiar contraseña" de ese correo fue quizás el error que desencadenó uno de los mayores golpes a la campaña de Hillary Clinton.

John Podesta acababa de entregar su contraseña genuina con un método de hackeo ampliamente conocido llamado "phishing" o suplantación de identidad. Desde junio de aquel año, Schultz denunció la intromisión, pues dijo que la firma de seguridad CrowdStrike, contratada por los demócratas.

La firma identificó dos grupos de atacantes, uno llamado Fancy Bear que acababa de entrar al sistema, y otro que llevaba allí casi un año y se denomina Cozy Bear. Ambos son nombres utilizados por un grupo de ciberespionaje vinculado al gobierno ruso que los investigadores del FBI han llamado The Dukes (los duques), explica desde Moscú el periodista Andrey Soshnikov, experto en temas de seguridad de BBC Rusia.

Pero quizás este "kompromat" pudo haberse evitado si el asesor de seguridad de los demócratas no hubiera cometido el error que le reconoció en entrevista a The New York Times: haber olvidado escribir un "not" en su respuesta en inglés a John Podesta.

Es decir, no haberle escrito "This is 'not' a legitimate email", en español: "Este 'no' es un correo legítimo".

CASO 2 BREXIT

Introducción: contexto del Brexit

Los ingleses votaron para abandonar la Unión Europea por mayoría simple el 23 de junio de 2016. El porcentaje de votantes se englobó alrededor del 72,2%, de los cuales el 51,9% optaron por abandonar la Unión, con 12,9 puntos de ventaja con respecto a los partidarios de la permanencia. Previamente, un referéndum celebrado en 1975 había ratificado la adhesión del Reino Unido que, por aquel entonces, era conocido como "Comunidad Económica Europea". Los partidarios del Brexit se posicionaron del lado antiliberal, esencialmente de manera populista y enarbolando el lema de "recuperen el control" sobre temas como inmigración, legislación, economía, comercio, pesca, etc. Los resultados del referéndum en el Reino Unido podrían entenderse como uno de los casos más paradigmáticos dentro del resurgimiento de fuertes nacionalismos y populismos. El apoyo a estos discursos no es único de un país ni el Reino Unido se quedó atrás. Igualmente, en colaboración con otros, parte del llamado "nuevo eje euroescéptico" también compartió intereses en la desunión europea y nacionalismos posteriores a la firma del Tratado Europeo de Lisboa. No obstante, estos grupos no siguieron estrategias legales y públicas en pos de sus intereses, sino que, extraoficial y subrepticiamente, han llegado a mostrar un fuerte interés por manipular datos públicos o divulgar una información parcial, tergiversada o directamente falsa en beneficio propio.

De acuerdo con Moresi, Motta, Trama, Walker y Amaya (2021), el Brexit generó múltiples implicancias en los ámbitos social, político y cibernético, cada uno de los efectos de la estabilidad y seguridad de Europa y el Reino Unido. Estos autores destacan que el ciberespacio y las tecnologías de información juegan un papel crucial de la manera en que se configuran los conflictos y las dinámicas de poder en una era marcada por la interconectividad. En términos sociales, la incertidumbre y fragmentación dentro del Reino Unido y Europa se intensificaron, con el ciberespacio como un canal que facilita la propagación de desinformación y polarización de opiniones, lo que puede exacerbar tensiones y manipular la percepción pública (Moresi et al., 2021, p.86)

Importancia e implicancias de la manipulación de datos

El Brexit exacerbó divisiones sociales y políticas en el Reino Unido y la Unión Europea (UE), impulsadas y amplificadas por campañas digitales. En el contexto de ciberdefensa, estas campañas son representativas del uso estratégico de la información para influir en la opinión pública y desestabilizar posiciones políticas a través de herramientas digitales como las redes sociales y campañas de desinformación. Las implicancias sociales en este sentido abarcan desde la pérdida de confianza pública en los sistemas de información hasta una fragmentación social basada en percepciones inducidas o manipuladas a nivel masivo.

En ese sentido, se observa una creciente importancia de la manipulación de datos en el terreno político, no solo por el ataque constante a ciertos grupos económicamente privilegiados o por la saturación informativa, sino por el creciente interés y papel transformador que las TIC juegan en la política en los últimos años y, con especial énfasis, en las últimas campañas electorales de varios países europeos. La manipulación de datos ha sido fundamental, sumado esto a las técnicas de desinformación mediática que utilizan grandes actores político-económicos municipales, regionales, estatales e internacionales. Las TIC son aplicadas con un alto nivel de politización y apuntan a estar contempladas también por los grandes grupos político-económicos. La manipulación de datos por parte de grupos en el contexto político contemporáneo. Los desarrollos tecnológicos no determinan el rumbo de un proceso social que estas acompañan, promueve una cultura política democrática cada vez más desvinculada de procesos efectivos de formación de opinión y propuestas, a favor de una cultura de la información sin virtudes democráticas. (Méndez Muros, 2021)

La manipulación de datos en el marco del ámbito de la publicidad política puede expresarse de diversas maneras. Así, pueden distinguirse las siguientes formas de manipulación de datos:

- Omitir algunas partes del fenómeno que se anuncia.
- No reconocer, anunciar o indicar una parte del fenómeno que no existe.
- Distorsionar lo realizado, hablar de él como si fuera otro.
- Utilizar una fórmula para medir un fenómeno como si fuera otro, aunque se diga que se está midiendo un tercero.
- No adecuar las fórmulas de comparación para ver con claridad cuál de los dos fenómenos indicados es más grande o más pequeño.
- Manipular las comparaciones o ilustraciones utilizando gráficos.

Por otro lado, en términos de seguridad de la información, el Brexit generó nuevos riesgos y alteró la dinámica de defensa compartida. La salida de los sistemas europeos implica que el Reino Unido debe reestructurar y reforzar su infraestructura de ciberdefensa independiente, tanto para protegerse contra ciberataques de actores estatales y no estatales como para contrarrestar campañas de influencia. El ciberespacio actúa como un dominio clave, ya que los países involucrados han experimentado un aumento en la actividad de ataques cibernéticos y desinformación, siendo estos nuevos vectores de conflictos menos tangibles, pero potencialmente igual de destructivos en cuanto a impacto social y económico. Por ello, el Brexit marcó un giro hacia políticas de ciberseguridad y defensa más independientes en el Reino Unido, y el distanciamiento de las estructuras de defensa de la Unión Europea exige reestructuraciones en la infraestructura cibernética y nuevos enfoques de inteligencia para mitigar ataques cibernéticos de actores estatales. y no estatal (Moresi et al., 2021). Esta transición resalta la necesidad de asegurar la infraestructura crítica y protegerla de amenazas cibernéticas que intentan desestabilizar la región, tanto mediante ataques directos como a través de operaciones de información que buscan influir en los procesos democráticos y la cohesión social.

Estrategias de manipulación de datos utilizados

Los resultados de las investigaciones demostraron que los defensores de la salida de Gran Bretaña de la Unión Europea utilizaron tres tácticas principales para manipular a la opinión pública. La primera fue proporcionar información falsa y utilizar algoritmos de aprendizaje automático para personalizar los mensajes, generando noticias falsas distribuidas en redes sociales, que de acuerdo con la mayoría de los encuestados contribuyeron al buen resultado del referéndum. La segunda fue emplear datos manipulados y extraer datos de fuentes privadas. Y finalmente, utilizar datos para dirigirse con eficiencia a los segmentos de la opinión pública increpados, y con el fin de maximizar el grado de segmentación se obtuvieron datos a través de micropagos en línea o cuestionarios en línea engañosos. (Tuñón Navarro, 2021)

Todas estas estrategias responden al uso de dos nuevos modelos de comunicación política internacionales y característicos del contexto político contemporáneo: las estrategias de campaña asimétricas y la microsegmentación electoral. Ambas operan a nivel micro y usan la recopilación y explotación de grandes bases de datos con el fin de conocer exhaustivamente a los electores o posibles electores para persuadirlos informáticamente y de manera individualizada. Algunas conclusiones de este trabajo afirman que en el contexto del Brexit las

tres principales armas persuasivas utilizadas por los pro-Brexit a través de la manipulación de datos provenientes de las redes sociales fueron el miedo, el nacionalismo y la oferta de soluciones fáciles, incluido el abuso del principio democrático. Además, tanto los ciudadanos como los agentes participantes fueron víctimas y/o cómplices de dichas prácticas. (Cerveró, 2021)

Desinformación y Propaganda en el Ciberespacio

Desde los orígenes del fenómeno de la seguridad y defensa, es importante conocer también las implicancias de la propaganda y la desinformación en los conflictos bélicos o estratégicos, brindándoles un peso mayor a los medios de comunicación. En el seno de una organización internacional, la OTAN, había conciencia del uso masivo del ciberespacio en distintas modalidades; entre ellas, contaba el uso estratégico de la doctrina de desarrollo, que era reconocido (Pérez, 2023).

Siguiendo a Moresi et al. (2021), los autores exponen cómo el Brexit también fue una oportunidad para actores externos, como Rusia, que ha sido acusada de influir en decisiones políticas clave en Europa, utilizando el ciberespacio como un "nuevo dominio del conflicto".

> Esto implica que el ciberespacio se convierte en un espacio de lucha donde los estados buscan alterar percepciones, desinformar y, en última instancia, modelar los comportamientos a favor de sus propios intereses (Moresi et al., 2021, p. 86)

Respuestas regulatorias y políticas

A medida que avanza el desarrollo tecnológico, surge la necesidad de regular el uso y tratamiento de datos personales por parte de terceros con el objetivo de garantizar los derechos individuales frente al abuso de datos sensibles, personales y privados. En este sentido, la regulación desempeña un papel esencial en el contexto político contemporáneo. En sus últimos años, muchos estados, desde el punto de vista legislativo, han llevado a cabo una serie de actuaciones encaminadas a hacer frente a las lagunas jurídicas que se han conocido y aprovechado en función de sus necesidades políticas.

Los expertos coinciden en buscar una regulación que pueda proteger de manera global los derechos de las personas, es decir, que exista una regulación universal. Tal es el caso del papel que juega la Unión Europea, con el nuevo Reglamento General de Protección de Datos; cumpliendo un punto de inflexión en el que se introduce un nuevo modelo de gobernanza que establece una mayor responsabilidad de las empresas y una disponibilidad de información más

clara sobre las prácticas de tratamiento de los datos personales. Para el resto del mundo, la normativa europea puede establecer las pautas que puede seguir para desarrollar sus modelos propios. (Roca, 2020)

Impacto en la confianza pública y la democracia

Dentro del contexto político contemporáneo, especialmente tras el escándalo, las empresas encargadas de hacer llegar los mensajes a través de la publicidad buscan aconsejar o ayudar a partidos políticos o movimientos con propuestas electorales que evidentemente son del interés del candidato o candidata o movimiento político. La aparición de los Big Data en este juego hace que se dedique un volumen de recursos sin precedentes en alcanzar a las personas gracias a las categorías que ellos mismos aportan, lo que permite identificar en cada momento el argumento o el mensaje que puede resultar más persuasivo y, una vez conseguidos el número de apoyos necesarios, buscar los votos de más que permitan formar un gobierno.

En el marco de esta puesta en escena, el resultado del referéndum fue la consecuencia de actuaciones políticas líderes y las técnicas políticas de manipulación en un clima político y social particular y puede ser considerado un caso ilustrativo de una tendencia política global de hacer política al margen de la verdad evidente, a la mentira o la desvinculación efectiva y emocional de las élites políticas. La utilización de las tecnologías de la información y la comunicación en general, y las redes sociales en particular, han sido señaladas por distintos actores y actrices como causantes y consecuentes con el referéndum, acusando de manipulación a aquellas iniciativas, particulares o no, que hicieron campaña a favor de la salida del Reino Unido de la Unión Europea.

Reacciones y consecuencias

El uso de bases de datos, las redes sociales o la automatización de procesos que usan análisis predictivos, aplicados con distintos objetivos tales como el seguimiento, la identificación o el influjo en las actitudes del votante hacia un partido o candidato concreto, entre otros, suponen una revolución en los métodos de comunicación de la política, pudiendo

generar efectos inspiradores, pero también peligrosos y desestabilizadores, especialmente en el contexto de debilitamiento de los partidos tradicionales.

En consecuencia, el Brexit y la campaña que lo hizo posible están cargados de manipulaciones de datos, desde falsedades a medias verdades, al más primario y puro engaño colectivo. Al igual que el referéndum, se reconoció un debate superficial y tendencioso. Lo que les ocurre a los británicos no es otra forma de democracia. La propaganda, sea jocosa o desafiante, graciosa o venenosa, no genera ciudadanos, deforma, no informa, manipula.

Los ciudadanos deben tener acceso a información transparente y precisa, sin someterse a manipulaciones engañosas. Solo así es posible asegurar un sistema democrático sólido y saludable, basado en la libre elección y en la toma de decisiones justas y racionales. Además, es necesario fomentar una cultura política en la que se valore y respete la diversidad de opiniones y se promueva el diálogo constructivo. Asimismo, los líderes políticos tienen la responsabilidad de actuar con integridad y honestidad, sin recurrir a estrategias manipuladoras para alcanzar sus objetivos.

En definitiva, el Brexit ha dejado al descubierto la fragilidad de la democracia y la facilidad con la que las masas pueden ser influenciadas por discursos engañosos. Es hora de aprender de nuestros errores y trabajar juntos para fortalecer nuestros sistemas políticos y garantizar un futuro más justo y equitativo para todos.

Tendencias emergentes

Tal como venimos trabajando en los apartados anteriores afirmamos que la forma en que se relacionan, interactúan, comunican, perciben y sienten las personas permite un cambio en el carácter de la guerra y, por ende, la aparición de un nuevo tipo de guerra: la guerra cognitiva. Aunque las estrategias de propaganda e influencia siempre han existido, la sofisticación de las nuevas tecnologías digitales y el uso cada vez más generalizado de las redes sociales han hecho posible que actores estatales, no estatales e independientes, lleguen a audiencias más amplias con contenido personalizado y en tiempo real a través de operaciones de influencia. La guerra cognitiva lleva enfoques conocidos y novedosos dentro de la información, la cibernética y la guerra psicológica a un nuevo nivel, al intentar no solo alterar la forma en que piensan las personas, sino también cómo reaccionan ante la información. Además, los métodos de guerra cognitiva desdibujan las líneas entre objetivos civiles y militares y podría decirse que cambian la aplicación de la fuerza de los dominios físicos a los virtuales tal como señala Douhet (2023).

> Todas las actuales tendencias emergentes de las operaciones de influencia se relacionan con las operaciones cibernéticas, en razón que comparten el mismo modus operandi o, peor aún, pueden emplear los mismos canales para la ejecución de sus acciones. En este sentido, las operaciones cibernéticas pueden emplear virus informáticos, los cuales se propagan a través de las redes sociales y están dirigidos a los contactos de la víctima, de manera tal que los agentes de operaciones de influencia utilizan la información de los contactos de la persona afectada para difundir una cantidad abrumadora de información falsa o engañosa, a través de cuentas que se ven e interactúan de forma humana (Bernal et al., 2020).

También vemos que las nuevas tendencias tienen una relación muy estrecha con el fenómeno de la urbanización de las naciones, que permite a las grandes urbes conectarse con las ciudades medianas y pequeñas, en lo que algunos autores clasifican como megaciudades. De esta manera, millones de personas se concentran en espacios reducidos y así se convierten en blancos potenciales de la guerra cognitiva/ operaciones de influencia. Si en el pasado los objetivos militares implicaban la conquista de vastos territorios, hoy las grandes ciudades y sus poblaciones, especialmente en los países en desarrollo, son el foco de atención de todo tipo de actores (Hoffman, 2007). Por consiguiente, tal concentración de población favorece un mayor alcance de las operaciones psicológicas y, por ende, las operaciones de influencia.

En resumen, en un ambiente cada vez más urbano, las operaciones psicológicas persiguen controlar lo que sienten las personas, las operaciones de información intentan controlar lo que ve la población objetivo y las operaciones cibernéticas pretenden interrumpir las capacidades tecnológicas de la mencionada población. Es decir, todas en conjunto aportan a la guerra cognitiva, la cual se enfoca en influir sobre cómo piensa y actúa la población objetivo, para finalmente desestabilizarla.

Otra tendencia emergente y no tratada en la Diplomatura es la postverdad y su relación con las operaciones de influencia. Hannan et al. (citado en Giusti y Piras, 2021) emplean la expresión posverdad para describir la compleja relación contemporánea en la que realidad, falsedad y poder interactúan y se mezclan en el mundo de los medios y las redes sociales. Para los mencionados autores, la posverdad:

> Revela una fase política en la que las personas se inclinan a aceptar argumentos basados en sus propias emociones y creencias más que en hechos y realidades. En consecuencia, decisiones políticas tan importantes como votar para elegir a sus gobernantes o la toma de decisiones colectivas como un referéndum, están más relacionadas con impulsos emocionales, ideológicos e impresiones superficiales más que a la selección racional basada en evaluaciones de políticas. El debilitamiento de la relevancia del razonamiento racional se abre a la fácil instalación de información falsificada. En esta perspectiva, una mentira no es necesariamente algo que se opone a la verdad; es más bien un derivado de una versión distorsionada de la misma, de modo que los límites entre la verdad y la mentira se difuminan (Giusti y Piras, 2021, p. 6, traducción propia).

Como lo explica Bufacchi (2020), mientras que una mentira subvierte una verdad específica, la posverdad intenta subvertir la verdad misma y el prefijo pos se refiere a la afirmación de que una idea específica se ha vuelto redundante y, por lo tanto, puede desecharse de forma segura. La posverdad es la creencia de que la verdad ya no es esencial, que la verdad se ha vuelto obsoleta. En este mismo sentido, Keller, Schoch, Stier y Yang (2020) añaden que las noticias falsas son una excelente herramienta para allanar el camino hacia la posverdad, ya que estas no necesariamente niegan los hechos o lo que se puede definir como verdad, sino que sugieren interpretaciones engañosas o inventan hechos que no existen pero que, sin embargo, son plausibles o cercanos a lo que el público podría esperar. De otra parte, Polyakova y Meserole (2019) afirman:

> Los Estados se han convertido en cuna de políticas divisorias a través de sus discursos y políticas populistas, la deslegitimación de la competencia, las políticas de odio y resentimiento, la demonización, la enemistad de sus adversarios políticos, y todos estos elementos se han vuelto rasgos comunes tanto en regímenes democráticos como autocráticos (p. 4, traducción propia).

En este sentido, un dirigente político podría usar la posverdad para dominar el escenario político o para deslegitimar a un oponente, sus ideas, la historia e incluso toda una ideología o cultura. Estas acciones las llevaría a cabo por medio de técnicas de política divisiva, empleando la combinación de tecnologías de la información, las redes sociales, las noticias falsas y la desinformación, de tal suerte que intoxicaría no solamente el ambiente político, sino también el social, para que los ciudadanos se vuelvan partidistas de un grupo en específico y se enfrenten al contrario (Polyakova y Meserole, 2019). Un ejemplo de cómo se ha aplicado la posverdad lo podemos tomar del mandato del expresidente Donald Trump y su política "América grande otra vez". A través de esta política, el exmandatario daba a entender a sus seguidores que Estados Unidos estaba en decadencia y él sería su salvador. Así mismo, esta política polarizó al país y exacerbó los sentimientos hacia los inmigrantes y las tensiones raciales en los Estados Unidos.

Con todo lo anteriormente expuesto, se podría decir que las nuevas tecnologías sumadas a las redes sociales han permitido la aparición y propagación de fenómenos como las noticias falsas, la desinformación y la posverdad, las cuales se convierten en nuevas amenazas para la seguridad y defensa nacional, de las que Argentina no ha estado exenta.

Para contrarrestar esto, es imprescindible generar en los gobernantes y comandantes militares la consciencia acerca de los riesgos silenciosos de las amenazas cognitivas e

informacionales, y también del conjunto de las capacidades no cinéticas que tienen a su disposición para hacer la prevención y el enfrentamiento de tales amenazas.

Para concluir este apartado señalamos el trabajo realizado por Douhet (2023) donde simplificó esta problemática existente en una tabla llamada “Confrontación ejemplificadora entre algunas amenazas cognitivas y capacidades institucionales de las Fuerzas Militares”.

Amenazas cognitivas	Capacidades institucionales	Posibilidades de enfrentamiento (ejemplos)
Fragmentación del tejido social	Sistema de comunicación social y sistemas de gestión y protección del patrimonio cultural e histórico	Campañas de fortalecimiento de la identidad nacional y los valores culturales
Desestabilización de las instituciones	Sistema de educación	Fortalecimiento de la cultura de legalidad y apoyo a las instituciones
Manipulación de las emociones colectivas	Sistema de comunicación social y sistemas de asistencia social	Fortalecimiento de comunicaciones estratégicas, creación de una sección dedicada a contrarrestar noticias falsas, posverdad y desinformación
Miedo de actuar por inseguridad jurídica	Sistemas de doctrina militar y asesoría jurídica	Ampliación y actualización de los manuales de procedimiento
Noticias falsas	Comunicaciones estratégicas	Creación de un noticiero institucional

Conclusión

Las operaciones de influencia y las operaciones de información son herramientas poderosas en el ciberespacio, con un impacto significativo en la seguridad y la estabilidad a nivel individual, social y político. Si bien comparten similitudes, también presentan diferencias en cuanto a su alcance, propósito y medios. En muchos casos, se complementan e integran en estrategias más amplias de ciberseguridad y defensa nacional.

Es crucial comprender la naturaleza y las implicaciones de ambas para poder desarrollar estrategias efectivas de defensa y respuesta, así como para promover la alfabetización digital y la resiliencia frente a la manipulación y la desinformación en el ciberespacio.

De hecho, la aparición del ciberespacio como un ámbito que forma parte inseparable de nuestras vidas ha traído consigo una amplia gama de problemas, desde el punto de vista de seguridad para los actores estatales. La situación que están viviendo los estados como consecuencia de ser atacados desde el mundo virtual es un fenómeno que requiere de abordaje y reflexión. Hoy en día, vivimos en un mundo en el que se intercambian cantidades masivas de datos que se utilizan para obtener información útil. La computadora es una herramienta esencial

para el análisis de datos, ya que es mucho más rápida y capaz de procesar más información de la que un ser humano puede manejar. Las estadísticas de hoy en día han ofrecido la oportunidad de persuadir a muchas personas sobre algo. Actualmente, la política y los datos están más relacionados.

A lo largo de estos años, el comportamiento social y comunicativo de los usuarios se ha incrementado notablemente, adquiriendo suma relevancia en el ámbito digital a escala local, nacional e internacional. El uso de campañas de desinformación de carácter político, conocidas como fake news, se ha subrayado especialmente en asuntos que revierten importantes cambios en el orden civil, como consecuencia, principalmente, de la utilización de datos personales de miles de personas que se facilitaron en el ejercicio de su autonomía e identidad digital.

La superioridad militar convencional de un país, al menos en el futuro inmediato, no garantizará vencer en este nuevo tipo de guerra y estos desafíos no se pueden enfrentar únicamente a través del uso del instrumento de poder militar de una nación. Lo ideal sería lograr anticipar el cambio del carácter de la guerra y diseñar la estrategia adecuada por medio de la articulación tanto de los instrumentos (diplomático, informacional, militar y económico) y elementos de poder nacional (capital humano, industria, economía, tecnología, investigación y desarrollo, infraestructura, cultura, gobernanza, deseo nacional y reputación internacional) para mantener a salvo los intereses nacionales.

Referencias

Bernal, A.; Carter, C.; Singh, I.; Cao, K. y Madreperla, O. (2020). Cognitive Warfare. An Attack on Truth and Thought. Johns Hopkins University y North Atlantic Treaty Organization.

Bufacchi, V. (2020). What's the Difference between Lies and Post-Truth in Politics? A Philosopher Explains. The Conversation. Recuperado de: https://theconversation.com/whats-the-difference-between-lies-and-post-truth-in-politicsa-philosopher-explains-130442

Cerveró, E. D. (2021). Los retos de la comunicación ante los escenarios de la realidad actual. Ed. Universidad Panamericana.

Douhet, G. (2023) La guerra cognitiva y nuevas formas de amenazas a la paz ya la seguridad y la defensa nacionales. Bogotá. Recuperado de https://doi.org/10.25062/9786287602489.14

García, C. S. (2023). Poderes fácticos y tecnologías disruptivas: hacia una democracia de la vigilancia basada en el dominio de las plataformas digitales. Revista del CLAD Reforma y Democracia. clad.org

Giusti, S. y Piras, E. [Eds.] (2021). Democracy and fake news: information manipulation and post-truth politics. Abingdon y Nueva York: Routledge.

Hoffman, F. G. (2007). Conflict in the 21st Century. Arlintong: The Potomac Institute for Policy Studies.

Keller, F. B.; Schoch, D.; Stier, S. y Yang, J. (2020). Political Astroturfing on Twitter: How to Coordinate a Disinformation Campaign. Political Communication, 37(2), 256-80. DOI: 10.1080/10584609.2019.1661888

Méndez-Muros, S. (2021). Aproximación a una metodología de análisis de las emociones en el discurso político televisado. Vol. 9. Investigación Cualitativa en Ciencias Sociales: Avances y Desafíos. New Trends in Qualitative Research. ludomedia.org

Moresi, A., Motta, G., Trama, GA, Walker, M. y Amaya, C. (2021). 14 CA XIV Operaciones en el Dominio de la Información. Facultad Militar Conjunta. Universidad de la Defensa Nacional.

Pérez, M. M. P. (2023). Usos, retos y oportunidades de la inteligencia artificial en el ejército. De Lege Ferenda. ugr.es

Polyakova, A. y Meserole, C. (2019). Exporting Digital Authoritarianism: The Russian and Chinese Models. Policy Brief, Foreign Policy at Brookings Institution. Recuperado de: https://www.brookings.edu/wp-content/uploads/2019/08/FP_20190827_ digital_authoritarianism_polyakova_meserole.pdf

Roca, A. P. (2020). El derecho a la protección de datos personales y su reflejo en el consentimiento del interesado. Revista de Derecho Político. uned.es

Tuñón Navarro, J. (2021). Manual de periodismo y verificación de noticias en la era de las Fake News. Desinformación y Fake News en la Europa de los populismos en tiempos de pandemia (Cap. X). uned.es

Ventre, D. (2016). Information warfare (La guerra de la Información). 2da. ed. USA. Ed Wiley.