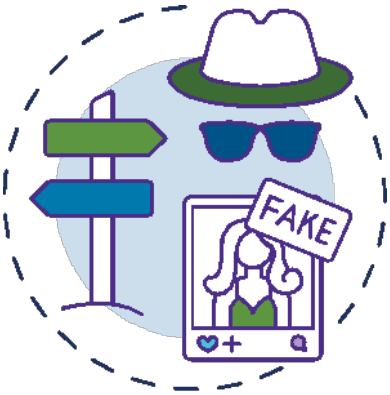
Tácticas de Desinformación

Los actores de desinformación utilizan diversas tácticas para influir en otros, incitarlos a actuar y causar daño. Comprender estas tácticas puede aumentar el nivel de preparación y promover la resiliencia al enfrentar la desinformación.

Si bien esta serie analiza ejemplos de fuente abierta de desinformación atribuida por otros a gobiernos extranjeros, no representa que gobierno de los EE. UU. confirma la exactitud de dicha atribución.



¿Qué son las tácticas de desinformación?

Los actores de desinformación utilizan diversas tácticas y técnicas para llevar a cabo operaciones de información y difundir narrativas de desinformación que representan un riesgo para la infraestructura crítica. Cada una de estas tácticas está diseñada para hacer que los mensajes de los actores de desinformación sean más creíbles o para manipular a su audiencia con un fin específico. A menudo buscan polarizar a su grupo objetivo divisiones políticas o polémicas sociales, haciendo que la audiencia sea más receptiva a la desinformación.

Estos métodos pueden y han sido utilizados como armas por actores de desinformación para así generar amenazas a la infraestructura crítica de los EE. UU. La serie Tácticas de Desinformación ayuda a las organizaciones a comprender y a manejar los riesgos que genera la desinformación al desglosar tácticas comunes, compartir ejemplos reales y proporcionar acciones concretas para contrarrestar dichas narrativas con información veraz. Cualquier organización, al igual que su personal pueden ser el objetivo de las campañas de desinformación, y todas las organizaciones tienen un papel que desempeñar en la construcción de un entorno de información resiliente. Este y otros productos disponibles en la Biblioteca de Recursos de CISA MDM, apoyan a las organizaciones de infraestructura crítica a evaluar su situación de riesgo y a desarrollar resiliencia en sus comunidades.

Descripción general de las tácticas

Mantener personas y sitios web falsos o engañosos: Los actores de desinformación crean redes con personas y sitios web falsos para aumentar la credibilidad de su mensaje en su público objetivo. Las redes de expertos falsos utilizan credenciales inauténticas (por ejemplo, "expertos" falsos, periodistas, grupos de expertos o instituciones académicas) para otorgar credibilidad indebida a su contenido influyente y hacerlo más creíble.

Crear ultrafalsos [*deepfakes*] y medios artificiales: El contenido de medios artificiales puede incluir fotos, videos y clips de audio que han sido manipulados digitalmente o fabricados en su totalidad para engañar al espectador. Las herramientas de inteligencia artificial (IA) pueden hacer que el contenido sintético sea casi indistinguible del real. El contenido de medios artificiales puede implementarse como parte de las campañas de desinformación para promover información falsa y manipular audiencias.

Idear o ampliar teorías: Las teorías de conspiración intentan explicar eventos importantes como tramas secretas de actores poderosos. Las teorías de la conspiración no solo afectan la comprensión que un individuo tiene sobre un tema en particular; ellas pueden dar forma e influir en toda su visión del mundo. Los actores de desinformación aprovechan al máximo las teorías de conspiración para generar narrativas de desinformación alineadas con la cosmovisión de la conspiración, lo que aumenta la probabilidad de que la narrativa resuene en el público objetivo.

***Astroturfing* e inundación del entorno de información:** Las campañas de desinformación a menudo publican cantidades inmensas de contenido con mensajes idénticos o similares provenientes de varias cuentas inauténticas. Esta práctica, conocida como *astroturfing*, crea la impresión de un amplio apoyo u oposición a un mensaje por parte de los grupos base, al tiempo que oculta su verdadero origen.

Una táctica similar, la inundación, consiste en enviar correos basura [*spam*] a las publicaciones de las redes sociales y a las secciones de comentarios, con la intención de dar forma a una narrativa o de minimizar puntos de vista opuestos.

Abuso de plataformas alternas: Los actores de desinformación pueden abusar de plataformas de redes sociales alternas para aumentar la creencia de grupos de usuarios específicos en una narrativa de desinformación.

Los actores de la desinformación pueden buscar aprovechar plataformas con menos protecciones para el usuario, políticas de moderación de contenido menos estrictas y menores controles para la detección y eliminación de contenido y cuentas inauténticas, que otras plataformas de redes sociales.

Aprovechar las brechas de información: Los vacíos de datos, o las brechas de información, ocurren cuando no hay suficiente información creíble para satisfacer una consulta de búsqueda. Los actores de desinformación pueden explotar estas brechas generando su propio contenido de influencia y sembrando el término de búsqueda en las redes sociales para alentar a las personas a buscarlo. Esto aumenta la probabilidad de que las audiencias encuentren contenido de desinformación sin resultados de búsqueda precisos o autorizados para refutarlo.

Manipular a los actores desprevenidos: Los actores de desinformación identifican a personas y organizaciones destacadas para ayudar a amplificar sus narrativas. Dichos objetivos a menudo no saben que están repitiendo la narrativa de un actor de desinformación o que la narrativa está destinada a manipular.

Difundir contenido específico: Los actores de desinformación producen contenido de influencia personalizado y que probablemente resuena con una audiencia específica en función de su visión del mundo y sus intereses.

Estos actores obtienen un estatus de información privilegiada e incrementan el número de sus seguidores en línea, lo cual puede hacer que los futuros esfuerzos de manipulación sean más exitosos. Esta táctica a menudo toma un enfoque de "juego largo" con el fin de difundir contenido específico en un margen amplio de tiempo para generar confianza y credibilidad dentro del público objetivo.

Acciones que usted puede tomar

Si bien las tácticas de desinformación están diseñadas para engañar y manipular, la evaluación crítica del contenido y la verificación de la información con fuentes confiables antes de decidir compartirla puede aumentar la resiliencia contra la desinformación y retrasar su propagación. Comparta estos consejos:

- **Reconozca el riesgo.** Comprenda cómo los actores de desinformación aprovechan estas tácticas para impulsar su agenda. Tenga cuidado con contenido manipulador que intente crear división.
- **Cuestione la fuente.** Evalúe críticamente el contenido y su origen para determinar si es confiable. Investigue las credenciales del autor, considere la intención de la fuente y verifique los hechos que lo respaldan.
- **Investigue el problema.** Realice una búsqueda exhaustiva e imparcial de los temas polémicos observando lo que las fuentes creíbles dicen y analizando otras perspectivas. Confíe en fuentes de información fidedignas, como sitios gubernamentales.
- **Piense antes de compartir.** Tome su tiempo. No haga clic inmediatamente para compartir el contenido que ve en línea. Compruebe primero los hechos. Parte de la desinformación más dañina se propaga rápidamente a través de publicaciones compartidas que buscan provocar una reacción emocional que nuble el pensamiento crítico.

TACTICAS DE DESINFORMACION:

Mantener personas y sitios web falsos o engañosos

Los actores de desinformación utilizan diversas tácticas para influir en otros, incitarlos a actuar y causar daño. Comprender estas tácticas puede aumentar el nivel de preparación y promover la resiliencia al enfrentar la desinformación.

Si bien esta serie analiza ejemplos de fuente abierta de desinformación atribuida por otros a gobiernos extranjeros, no representa que gobierno de los EE. UU. confirma la exactitud de dicha atribución.

Descripción

Los actores de desinformación crean redes de personas y sitios web falsos para aumentar la credibilidad de su mensaje con su audiencia objetivo. Tales redes pueden incluir falsos “expertos” académicos o profesionales, periodistas, grupos de expertos y/o instituciones académicas. Algunas personas falsas incluso pueden validar sus cuentas de redes sociales (por ejemplo, una marca de verificación azul o gris junto a un nombre de usuario), lo que confunde aún más a las audiencias acerca de su autenticidad. Las redes de expertos falsos usan credenciales inauténticas para hacer que su contenido sea más creíble.

Los actores de desinformación también aumentan la credibilidad de estas personas falsas al generar artículos o trabajos de investigación falsificados y compartirlos en línea. A veces, estas personas y las publicaciones asociadas con ellas son intencionalmente amplificadas por otros actores. En algunos casos, estos materiales también son compartidos por organizaciones y usuarios legítimos sin darse cuenta. La creación o amplificación del contenido de estas personas falsas dificulta que el público distinga a los verdaderos expertos de los falsos.

Con esta táctica los adversarios también han demostrado un enfoque de "juego largo" al generar seguidores y credibilidad con contenido aparentemente inocuo antes de cambiar su enfoque a la creación y amplificación de la desinformación. Esto les proporciona una falsa credibilidad a las campañas.

Ejemplos

- La agencia de inteligencia militar de Rusia, GRU, utilizó expertos falsos en sus esfuerzos para influenciar las elecciones presidenciales de EE. UU. en 2016. Los operativos de GRU crearon grupos de expertos falsos y sitios de noticias con artículos de personas inauténticas. Establecieron docenas de páginas públicas de Facebook para publicar y ampliar el contenido. El contenido varió desde expresar apoyo a los intereses rusos en los conflictos de Siria y Ucrania de 2014, hasta cuestiones de justicia racial en los Estados Unidos.[1]
- La red de sitios web falsos y de personas alineadas con Irán y conocida como "Endless Mayfly" se hace pasar por medios de comunicación legítimos para difundir narrativas de desinformación. Luego usan dichos personajes falsos para amplificar el contenido en las redes sociales.[2]

[1]DiResta, Renee y Shelby Grossman. Potemkin Pages & Personas: evaluación de las operaciones en línea de GRU, 2014-2019. Stanford, CA: Universidad de Stanford, 2019.
[2]Lim et al. Quemado después de leer: la campaña de desinformación efímera de Endless Mayfly. The Citizen Lab, 2019

Llamados a la acción

- Tanto en actividades de comunicación tradicionales como en redes sociales, dirija a las audiencias a sitios web oficiales y fuentes de información confiables.
- Asegurarse de que el sitio web de su organización transmita información clara, concisa y actual a la que las personas puedan acudir como una fuente confiable.
  Las organizaciones gubernamentales deben hacer la transición de los sitios web al dominio de nivel superior .gov para comunicar al público que el sitio web es genuino y seguro.
- Mantener actualizada la información en línea de la organización y “validar” las cuentas de redes sociales de la organización, representantes clave y voceros.
- Verificar las fuentes de artículos, documentos y otros recursos antes de compartirlos.

TACTICAS DE DESINFORMACION:

Crear ultrafalsos [*deepfakes*] y medios artificiales

Los actores de desinformación utilizan diversas tácticas para influir en otros, incitarlos a actuar y causar daño. Comprender estas tácticas puede aumentar el nivel de preparación y promover la resiliencia al enfrentar la desinformación.

Si bien esta serie analiza ejemplos de fuente abierta de desinformación atribuida por otros a gobiernos extranjeros, no representa que gobierno de los EE. UU. confirma la exactitud de dicha atribución.

Descripción

El contenido de medios artificiales puede incluir fotos, videos y clips de audio que han sido manipulados digitalmente o fabricados en su totalidad para engañar al espectador. Las falsificaciones baratas [*Cheapfakes*] son una forma de manipulación menos sofisticada que involucra clips de audio o videos reales que han sido acelerados, ralentizados o presentados fuera de contexto con el fin de engañar. Por el contrario, los ultrafalsos [*Deepfakes*] se desarrollan entrenando algoritmos de inteligencia artificial (IA) con contenido de referencia hasta que puedan producir multimedia casi indistinguible a la realidad. La tecnología *deepfake* hace posible representar de manera convincente a alguien haciendo algo que no ha hecho, o diciendo algo que no ha dicho. Si bien la tecnología de medios artificiales no es inherentemente maliciosa, puede utilizarse como un componente en las campañas de desinformación con el fin de compartir información falsa o de manipular audiencias.

Las fotos falsas creadas por actores de desinformación pueden ser utilizadas para generar imágenes de perfil realistas usadas para crear una gran red de cuentas de redes sociales inauténticas. Los videos falsos a menudo usan tecnología de inteligencia artificial para trazar el rostro de una persona en el cuerpo de otra. En el caso de ultrafalsos de audio, un “clon de voz” puede producir oraciones nuevas sea solo como audio o como parte de un ultrafalso en video, a menudo con solo unas pocas horas (o incluso minutos) de clips de audio de referencia. Finalmente, un uso emergente de la tecnología *deepfake* involucra texto generado por IA, que puede producir contenido escrito casi real, lo cual presenta un desafío único debido a su facilidad de producción.

Ejemplos

- La red de spam político pro-China Spamouflage Dragon usó perfiles generados por IA para crear un grupo de perfiles inauténticos para difundir sus videos falsos baratos en inglés que atacaban la política de los EE. UU en junio de 2020. Muchos videos mostraban cubrimiento de noticias con voces y subtítulos sobrepuestos.[1]
- En septiembre de 2020, Facebook eliminó trece cuentas atribuidas a la Agencia Rusa de Investigación de Internet que usaban imágenes de perfil generadas por IA para parecer más creíbles a las audiencias.[2]
- Los medios rusos promocionaron un video falso que supuestamente mostraba al presidente ucraniano Volodymyr Zelenskyy diciéndoles a las tropas ucranianas que se retiraran en marzo de 2022. Los piratas informáticos lograron transmitir el video en las noticias de televisión en vivo en Ucrania.[3]

Llamados a la acción

- Educar al personal sobre cómo su información personal (como fotos o videos públicos en las redes sociales) podría usarse para generar contenido de medios sintéticos y fomentar buenas prácticas de higiene cibernética en cuentas personales y profesionales.
- Utilizar herramientas disponibles públicamente, como la búsqueda inversa de imágenes, para verificar la fuente del contenido multimedia.
- Añadir descargos de responsabilidad al contenido que comparte o crea que incluya medios artificiales, incluso usos inocuos, para aumentar la conciencia pública.
- Incorporar la respuesta a videos ultrafalsos o clips de audio que afecten a su organización en el plan de respuesta a incidentes de su organización.
- Identificar rápidamente cualquier medio artificial que afecte a su organización o su mensaje y aclárelo en los canales oficiales, ofreciendo pruebas, de ser posible.

[1] Nimmo, Ben, Camille François, C. Shawn Eib y Léa Ronzaud. "Spamouflage va a Estados Unidos". Graphika, agosto de 2020. https://public-assets.graphika.com/reports/graphika_report_spamouflage_goes_to_america.pdf.
[2] Nimmo, Ben, Camille François, C. Shawn Eib y Léa Ronzauc. "IRA otra vez: trece desafortunados". Graphika, septiembre de 2020. https://public-assets.graphika.com/reports/graphika_report_ira_again_unlucky_thirteen.pdf.
[3] Allyn, Bobby. "El video falso de Zelenskyy podría ser la 'punta del iceberg' en la guerra de la información, advierten los expertos". NPR. NPR, 17 de marzo de 2022. https://www.npr.org/2022/03/16/1087062648/deepfake-video-zelenskyy-experts-war-manipulation-ukraine-russia.

TACTICAS DE DESINFORMACION:

Idear o ampliar teorías de conspiración

Los actores de desinformación utilizan diversas tácticas para influir en otros, incitarlos a actuar y causar daño. Comprender estas tácticas puede aumentar el nivel de preparación y promover la resiliencia al enfrentar la desinformación.

Si bien esta serie analiza ejemplos de fuente abierta de desinformación atribuida por otros a gobiernos extranjeros, no representa que gobierno de los EE. UU. confirma la exactitud de dicha atribución.

Descripción

Las teorías de la conspiración intentan explicar eventos importantes como tramas secretas de actores poderosos.[1] Las teorías de la conspiración no solo afectan la comprensión de un individuo sobre un tema en particular; pero también pueden dar forma e influir en toda su visión del mundo. Las teorías de la conspiración a menudo presentan una atractiva realidad alterna, al explicar eventos inciertos de una manera simple y aparentemente cohesiva, especialmente en momentos de mayor incertidumbre y ansiedad.

Los actores de desinformación aprovechan las teorías de conspiración para generar narrativas de desinformación que se alinean con la cosmovisión de la conspiración, lo cual aumenta la probabilidad de que la narrativa resuene en el grupo objetivo. Al repetir ciertos mensajes en múltiples narrativas, dichos actores aumentan la familiaridad de la audiencia con la narrativa y, por lo tanto, su credibilidad.

Las teorías de la conspiración también pueden ser un camino para la radicalización hacia la violencia entre ciertos adherentes. Las teorías de la conspiración pueden alterar la cosmovisión fundamental de una persona y pueden ser muy difíciles de contrarrestar retroactivamente, por lo que el desarrollo de resiliencia proactiva es especialmente crítico para evitar que el pensamiento conspirativo se arraigue.

Ejemplos

- En 2020, los canales de los medios estatales chinos y los funcionarios del gobierno afirmaron que el COVID-19 se había originado en los Estados Unidos y que un miembro del ejército estadounidense lo había llevado a China. Las narrativas estuvieron presentes al inicio entre las comunidades de conspiración en línea, pero las extensas redes de operaciones de información de China legitimaron y amplificaron estas narrativas en los medios tradicionales y sociales con el fin de redirigir las críticas del manejo del brote en China e intentar desacreditar a sus rivales geopolíticos.[2]

- El Ministerio de Defensa de Rusia desplegó la narrativa de desinformación de que el gobierno de EE. UU. está financiando programas militares en Ucrania para producir armas biológicas. Ampliadas aún más por el Ministerio de Relaciones Exteriores de China, estas narrativas buscan justificar la invasión de Rusia como una misión para neutralizar las supuestas armas biológicas y proporcionar motivos para culpar a EE. UU. o Ucrania en una posible operación de bandera falsa.[3]

Llamados a la acción

- Utilizar la Guía de respuesta a incidentes y planificación de MDM para preparar a su equipo para responder a posibles narrativas.
- Asegurarse de que el sitio web de su organización esté actualizado con información clara y precisa, incluida una página de preguntas frecuentes o Control de Rumores que aborde los puntos comunes de confusión sobre su trabajo.
- Establecer canales en línea y fuera de línea para compartir información con sus pares y socios y colabore como una red amplificadora para obtener información confiable.
- Educar de manera proactiva a las audiencias sobre cómo funcionan las teorías de la conspiración y los mensajes comunes que pueden encontrar.

[1] Douglas, Karen M, Robbie M Sutton y Alexandra Cichocka. "La psicología de las teorías de la conspiración". Direcciones actuales en ciencia psicológica 26, no. 6 (diciembre de 2017): 528–42. https://doi.org/10.1177/0963721417718261.

[2] DiResta, Renée. "Para China, el 'virus de EE. UU.' es una estratagema geopolítica". El Atlántico. Atlantic Media Company, 14 de mayo de 2020. https://www.theatlantic.com/ideas/archive/2020/04/chinas-covid-19-conspiracy-theories/609772/.

[3] Ascendente, David. "China amplifica la afirmación rusa no respaldada de los laboratorios biológicos de Ucrania". AP Noticias. Associated Press, 11 de marzo de 2022. https://apnews.com/article/russia-ukraine-covid-health-biological-weapons-china-39eeee023efdf7ea59c4a20b7e018169.

TACTICAS DE DESINFORMACION:

Astroturfing e inundación del entorno de información

Los actores de desinformación utilizan diversas tácticas para influir en otros, incitarlos a actuar y causar daño. Comprender estas tácticas puede aumentar el nivel de preparación y promover la resiliencia al enfrentar la desinformación.

Si bien esta serie analiza ejemplos de fuente abierta de desinformación atribuida por otros a gobiernos extranjeros, no representa que gobierno de los EE. UU. confirma la exactitud de dicha atribución.

Descripción

Las campañas de desinformación a menudo publican cantidades inmensas de contenido con mensajes idénticos o similares provenientes de varias cuentas inauténticas, sean estos creados por programas automatizados conocidos como 'bots' o por grupos profesionales de desinformación conocidos como 'granja de troles' [*troll farms*].Esta práctica, conocida como *astroturfing*, crea la impresión de un amplio apoyo u oposición a un mensaje por parte de los grupos base, al tiempo que oculta su verdadero origen.

Una táctica similar, la inundación, consiste en enviar correos basura [*spam*] a las publicaciones en las redes sociales y a las secciones de comentarios, con la intención de dar forma a una narrativa o de minimizar puntos de vista opuestos, a menudo utilizando muchas cuentas falsas y/o automatizadas. La inundación es también conocida como "manguera contra incendios".

Esta táctica se utiliza para sofocar el debate legítimo, como la discusión de una nueva política o iniciativa, y para disuadir a las personas de participar en espacios en línea. Quienes manipulan la información utilizan la inundación para entorpecer la sensibilidad de sus sujetos a través de la repetición y creando la sensación de que nada es cierto. Los investigadores denominan estas tácticas "censura por ruido", donde las narrativas amplificadas artificialmente intentan ahogar todos los otros puntos de vista.

La inteligencia artificial y otras tecnologías avanzadas permiten el despliegue de *astroturfing* y de inundaciones a gran velocidad y escala, manipulando más fácilmente el entorno de información e influyendo en la opinión pública.

Ejemplos

- En 2016, agentes rusos, parte de la Agencia de Investigación de Internet, se hicieron pasar por activistas de ambos lados del espectro político para inundar los canales de las redes sociales con contenido incendiario, así como para llamar a los activistas a asistir a eventos.[1]

- Se sospecha que el gobierno chino contrató hasta dos millones de personas, conocidas como el "Partido de los 50 centavos", para inundar la web en China con mensajes a favor del régimen. El Partido de los 50 centavos acalla a los críticos y distrae la atención de las cuestiones políticas al compartir una inmensa cantidad de noticias positivas en las plataformas en línea.[2]

[1]Keller et al. No es fácil detectar desinformación en Twitter. Esto es lo que aprendimos de 8 campañas políticas de 'astroturfing'. The Washington Post, 2019.
[2]King, Gary, Jennifer Pan y Margaret E. Roberts. Cómo el gobierno chino fabrica publicaciones en las redes sociales para una distracción estratégica, no para un argumento comprometido. Universidad de Harvard, 2017.

Llamados a la acción

- Si se sospecha que una cuenta no es auténtica, verifique detalles como la fecha de creación de la cuenta, la foto de perfil, la biografía, las cuentas seguidas o la actividad de publicación.
- Considerar si el contenido es publicado por cuentas sospechosas de bot o troll antes de compartirlo.
- Desarrollar una red de comunicadores confiables en su área para ampliar información fidedigna y precisa.
- Comunicarse con su audiencia a través de más de un canal, de modo que tenga formas alternas de compartir información si su organización es el objetivo de una campaña de inundación o *astroturfing*.
- Fomentar la discusión, el debate y la retroalimentación de sus electores tanto en foros en línea como fuera de ella.

TACTICAS DE DESINFORMACION:

Abuso de plataformas alternas

Los actores de desinformación utilizan diversas tácticas para influir en otros, incitarlos a actuar y causar daño. Comprender estas tácticas puede aumentar el nivel de preparación y promover la resiliencia al enfrentar la desinformación.

Si bien esta serie analiza ejemplos de fuente abierta de desinformación atribuida por otros a gobiernos extranjeros, no representa que gobierno de los EE. UU. confirma la exactitud de dicha atribución.

Descripción

Los actores de desinformación a menudo buscan oportunidades para que sus narrativas ganen tracción entre audiencias más pequeñas antes de intentar volverse virales. **Si bien las plataformas alternas de redes sociales no son inherentemente maliciosas**, los actores de desinformación pueden aprovechar las políticas de plataforma menos estrictas para aumentar la creencia de grupos de usuarios específicos en una narrativa de desinformación. Estas políticas pueden incluir menos protecciones para el usuario, políticas de moderación de contenido menos estrictas y menores controles para la detección y eliminación de contenido y cuentas inauténticas, que otras plataformas de redes sociales.[1]

Las plataformas alternas a menudo promueven discusiones no moderadas y el poder para almacenar/compartir archivos, lo cual es inherentemente malicioso, pero puede ser atractivo para los actores que desean compartir desinformación.* Si bien algunas plataformas alternativas prohíben la promoción de violencia en los canales públicos, es posible que tengan menos visibilidad en los canales privados o en los grupos que promueven violencia. Los grupos en plataformas alternas pueden operar sin la capacidad de escrutinio o detección que otras plataformas poseen. A menudo, los grupos se enfocan en temas o actividades específicas para generar confianza en la audiencia y los actores de desinformación pueden, a su vez, abusar de esa confianza para establecer credibilidad en otras plataformas.

Ejemplos

- El gobierno ruso ha alentado a los usuarios a recurrir a plataformas específicas para contenido pro-Kremlin de medios afiliados al estado, incluidos Sputnik y RT News. Estos canales difunden desinformación encubierta como falsos "corresponsales de guerra" o "verificadores de hechos" acerca de la invasión rusa en Ucrania.[2]

- Las organizaciones terroristas extranjeras ocasionalmente aprovechan las tácticas de desinformación para abusar también de las plataformas alternas. Organizaciones terroristas como ISIS han aprovechado las plataformas para difundir contenido malicioso, reclutar nuevos seguidores y coordinar actividades. La investigación muestra que las comunicaciones de ISIS en plataformas alternativas desempeñaron un papel en el aumento de los ataques terroristas en Europa entre 2015 y 2016.[3]

Llamados a la acción

- Fomentar las preguntas, los comentarios y el diálogo de sus seguidores y electores a través de los canales de comunicación.
- Capacitar al personal para responder preguntas y comentarios externos con información clara y precisa y empatía.
- Rotar las responsabilidades para responder a audiencias externas para evitar el agotamiento entre el personal.
- Trabajar con su equipo para desarrollar pautas comunitarias y expectativas de comportamiento en los canales de redes sociales y comuníqueselas a sus seguidores.
- De ser possible, trabajar abaje con socios que tengan presencia en diferentes canales de comunicación para permitir el rápido intercambio y amplificación de información.

[1]Greenhalgh, Spencer, Daniel G. Krutka, and Shannon M. Oltmann. "Gab, Parler, and (Mis)educational Technologies: Reconsidering Informal Learning on Social Media Platforms." *The Journal of Applied Instructional Design* 10, no. 3 (2021).
[2]Alazab, Mamoun and Kat Macfarlane. "Why Telegram became the go-to app for Ukrainians—despite being rife with Russian disinformation." *The Conversation* (2022).
[3]Walther, Samantha and Andrew McCoy. "US extremism on Telegram: Fueling disinformation, conspiracy theories, and accelerationism." *Perspectives on Terrorism* 15, no. 2 (2021).
**Nota: El uso indebido de las redes sociales por parte de un actor de desinformación no debe atribuirse a la plataforma de redes sociales, en ausencia de hechos articulables específicos tendientes a mostrar que la plataforma está actuando bajo la dirección o el control de un actor de desinformación.*

TACTICAS DE DESINFORMACION:

Aprovechar las brechas de información

Los actores de desinformación utilizan diversas tácticas para influir en otros, incitarlos a actuar y causar daño. Comprender estas tácticas puede aumentar el nivel de preparación y promover la resiliencia al enfrentar la desinformación.

Si bien esta serie analiza ejemplos de fuente abierta de desinformación atribuida por otros a gobiernos extranjeros, no representa que gobierno de los EE. UU. confirma la exactitud de dicha atribución.

Descripción

Los vacíos de datos, o lagunas de información, ocurren cuando no hay suficiente información creíble para satisfacer una consulta de búsqueda, como cuando un término deja de usarse o cuando un tema o evento emergente gana prominencia por primera vez (p. ej., noticias de última hora).

Cuando un usuario busca el término o frase, los únicos resultados disponibles pueden ser falsos, engañosos o tener poca credibilidad. Si bien los motores de búsqueda trabajan para mitigar este problema, los actores de desinformación pueden explotar esta brecha generando su propio contenido de influencia y sembrando el término de búsqueda en las redes sociales para alentar a las personas a buscarlo.

Debido a que los términos específicos que crean vacíos de datos son difíciles de identificar de antemano, las fuentes de información confiables a menudo no pueden mitigar de manera proactiva sus impactos con información precisa. Los actores de desinformación pueden explotar los vacíos de datos para aumentar la probabilidad de que un objetivo encuentre desinformación sin información precisa para el contexto, lo que aumenta la probabilidad de que el contenido se considere verdadero o fidedigno.[1] Además de esto, las personas a menudo perciben la información que encuentran en los motores de búsqueda como más creíble, y puede ser un desafío revertir los efectos de la desinformación una vez aceptada.

Ejemplo

- En 2015, como parte de su esfuerzo por socavar a los oponentes en la Guerra Civil Siria, Rusia explotó vacíos de datos para asociar falsamente una organización humanitaria siria con el terrorismo. Un pequeño número de fuentes respaldadas por Rusia, incluidos los medios de comunicación estatales, generaron cientos de artículos que fueron ampliados aún más por las redes de desinformación rusas en las redes sociales, inundando a los motores de búsqueda con contenido influyente.
  Las personas que buscaban información sobre la organización se encontraron con muchas narrativas que impulsaban la agenda de Rusia, lo que abrumó las fuentes de información autorizadas y precisas que aparecían más abajo en los resultados de búsqueda.[2]

[1]Golebiewski, Michael y Danah Boyd. "Vacíos de datos: donde los datos faltantes pueden explotarse fácilmente". Datos y sociedad, 29 de octubre de 2019. https://datasociety.net/wp-content/uploads/2018/05/Data_Society_Data_Voids_Final_3.pdf.

[2] Sohn, Olivia. "Cómo los Cascos Blancos de Siria se convirtieron en víctimas de una máquina de propaganda en línea". El guardián. Guardian News and Media, 18 de diciembre de 2017. https://www.theguardian.com/world/2017/dec/18/syria-white-helmets-conspiracy-theories.

Llamados a la acción

- Revisar el análisis del sitio web para ver qué términos usan las personas para mostrar el sitio web de su organización en los motores de búsqueda.
- Considerar de manera proactiva los hashtags y los temas de tendencia en las redes sociales para identificar las narrativas emergentes que pueden ser explotadas por los vacíos de datos.
- Hacer la de los sitios web oficiales del gobierno al dominio de nivel superior.gov y buscar la verificación de las cuentas oficiales de las redes sociales para comunicarle a su audiencia que su organización es una fuente confiable de información.
- Utilizar técnicas de optimización de motores de búsqueda para aumentar la visibilidad de su sitio web en los resultados de búsqueda.

TACTICAS DE DESINFORMACION:

Manipular a actores desprevenidos

Los actores de desinformación utilizan diversas tácticas para influir en otros, incitarlos a actuar y causar daño. Comprender estas tácticas puede aumentar el nivel de preparación y promover la resiliencia al enfrentar la desinformación.

Si bien esta serie analiza ejemplos de fuente abierta de desinformación atribuida por otros a gobiernos extranjeros, no representa que gobierno de los EE. UU. confirma la exactitud de dicha atribución.

Descripción

Las campañas de desinformación se dirigen a personas y organizaciones destacadas para ayudar a amplificar sus narrativas.
Estos difusores secundarios de narrativas de desinformación agregan credibilidad percibida a los mensajes y ayudan a sembrar estas narrativas a nivel de la base mientras ocultan su fuente original. Dichos objetivos a menudo no saben que están repitiendo la narrativa de un actor de desinformación o que la narrativa está destinada a manipular. El contenido está diseñado para apelar a sus emociones y las de sus seguidores, lo que hace que los *influencers* se conviertan en facilitadores involuntarios de campañas de desinformación.

Ejemplos

- En 2016, la Agencia Rusa de Investigación de Internet llevó a cabo una campaña para difundir contenido divisivo y reclutó de forma encubierta a estadounidenses de todo el espectro político para, sin saberlo, amplificar este contenido. Luego, nuevamente en 2020, la Agencia Rusa de Investigación de Internet desplegó una campaña para reclutar de manera encubierta a periodistas involuntarios para que escribieran freelance para medios de comunicación inventados.[1]
- En agosto de 2021, Facebook eliminó varias cuentas conectadas a una empresa de marketing del Reino Unido para sus operaciones vinculadas a Rusia. A partir de 2020, se crearon varias cuentas falsas y comenzaron a publicar memes y comentarios que afirmaban que la vacuna AstraZeneca COVID-19 convertiría a los destinatarios en chimpancés. Los hashtags y peticiones asociados con estas cuentas fueron luego compartidos por varios *influencers* de salud y bienestar. La firma del Reino Unido supuestamente también se puso en contacto con personas influyentes en YouTube, Instagram y TikTok para pedirles que impulsaran el contenido contra las vacunas. para pago.[2]
- Tras el “boicot diplomático” de los Estados Unidos a los Juegos Olímpicos de Invierno de 2022 en Beijing, China contrató a una empresa de relaciones públicas con sede en los EE. UU. para reclutar discretamente a personas influyentes en las redes sociales en los EE. UU. para amplificar los mensajes positivos, incluida la desinformación, sobre China y la competencia. Se eligieron personas influyentes para llegar a los segmentos de audiencia objetivo con contenido que se desvía de las denuncias de abusos contra los derechos humanos en China. Muchas publicaciones no atribuyeron correctamente su patrocinio, una violación de los requisitos de la plataforma que aumentó la credibilidad del contenido aparentemente orgánico.[3]

Llamados a la acción

- Educar a los líderes de la organización sobre cómo su presencia personal y profesional en las redes sociales puede ser objeto de difusión de desinformación.
- Proteger a las audiencias contra las campañas de desinformación de base al desacreditar o "pre-desacreditar" de manera proactiva las posibles narrativas de desinformación relacionadas con su trabajo.
- Animar a los seguidores a verificar las fuentes y evaluar antes de compartir más contenido en las redes sociales.

[1] Nimmo, Ben, Camille Francois, C. Shawn Eib y Lea Ronzaud. Rep. IRA otra vez: trece desafortunados: Facebook elimina una pequeña red creada recientemente vinculada a la agencia de investigación de Internet. Graphika, 2020.

[2] Elizabeth Culliford, Facebook elimina la red rusa que se dirigía a personas influyentes para vender mensajes contra las vacunas. Reuters, 2021

[3] Seitz, Amanda, Mike Catalini y Eric Tucker. "China usó la televisión, TikTok protagoniza la campaña discreta de los Juegos Olímpicos". AP NOTICIAS. Associated Press, 8 de abril de 2022. https://apnews.com/article/entertainment-technology-business-sports-travel-ebd23980015ffa35b60dbb0348e9ca62.

TACTICAS DE DESINFORMACION:

Difundir contenido específico

Los actores de desinformación utilizan diversas tácticas para influir en otros, incitarlos a actuar y causar daño. Comprender estas tácticas puede aumentar el nivel de preparación y promover la resiliencia al enfrentar la desinformación.

Si bien esta serie analiza ejemplos de fuente abierta de desinformación atribuida por otros a gobiernos extranjeros, no representa que gobierno de los EE. UU. confirma la exactitud de dicha atribución.

Descripción

Los actores de desinformación vigilan una comunidad en línea específica para comprender su visión del mundo, sus intereses y sus influenciadores clave y luego intentan infiltrarse publicando contenido de influencia personalizado que probablemente resuene entre sus miembros. Al comenzar con publicaciones entretenidas o no controvertidas que son aceptables para las comunidades objetivo, los actores de desinformación obtienen el estatus de "información privilegiada" y aumentan el número de seguidores en línea que pueden hacer que los futuros esfuerzos de manipulación sean más exitosos. Esta táctica se puede usar en combinación con el cultivo de expertos falsos, que difunden contenido específico en un margen amplio de tiempo, adoptando un enfoque de "juego largo" que otorga una falsa credibilidad a la campaña. El contenido dirigido a menudo toma formas altamente compartibles, como memes o videos, y puede llegar a audiencias muy específicas mediante métodos como publicidad paga y algoritmos de redes sociales explotados.

Ejemplos

- En su esfuerzo por sembrar división dentro de los Estados Unidos durante las elecciones presidenciales de 2016, la Agencia Rusa de Investigación de Internet (IRA) desplegó una vasta red de cuentas, páginas y grupos de redes sociales inauténticos para dirigirse a comunidades estadounidenses específicas, incluidos grupos raciales y étnicos, y pertenecientes a movimientos políticos o ideologías específicas. Por ejemplo, el IRA intentó desalentar la participación de los estadounidenses de raza negra en el proceso electoral mediante la creación de un ecosistema de cuentas falsas conectadas que se hacían pasar por medios de comunicación. La red de cuentas falsas impulsó narraciones repetitivas y, a veces, manipuló a personas influyentes legítimas para ampliar su contenido, dándole la apariencia de un estado interno dentro de la comunidad.[1]
- Una extensa red a favor de China de cuentas en línea inauténticas ha ampliado sus esfuerzos para dirigirse a audiencias globales en los últimos años. La operación se ha extendido a docenas de plataformas sociales y sitios web, incluidos foros alternativos que atienden a audiencias específicas, y ha desplegado contenido de desinformación en al menos siete idiomas, tales como ruso y español. Al igual que los esfuerzos de IRA, muchas de las cuentas en la red pro-China compartieron el mismo contenido y se vincularon a cuentas dentro de la red en otras plataformas. El contenido dirigido a menudo busca estimular acción en el mundo real. Por ejemplo, en abril de 2020, el contenido dirigido a los estadounidenses de origen asiático buscó movilizar protestas dentro de los EE. UU. contra los hallazgos de que el COVID-19 se originó en China.[2]

Llamados a la acción

- Comprender cómo su audiencia recibe información, incluidas plataformas y fuentes confiables.
- Evaluar la desinformación previa que ha afectado a su sector y otras posibles vulnerabilidades.
- Comunicar información precisa de manera clara y creativa a través de canales y medios que atraigan a segmentos específicos de su audiencia.
- Invertir en contenido claro y conciso en los sitios web oficiales para que sirva como información de referencia precisa y verificada. Dirija a los usuarios a este contenido si surgen campañas de desinformación y asegúrese de que las preguntas clave de las partes interesadas se aborden en un lenguaje y marco centrados en el usuario.
- Desarrollar un plan de respuesta a incidentes para mitigar el impacto de narrativas significativas de desinformación.

[1]DiResta, Renee, Kris Shaffer, Becky Ruppel, David Sullivan, Robert Matney, Ryan Fox, Jonathan Albright y Ben Johnson. "Las tácticas y tropos de la Agencia de Investigación de Internet". DigitalCommons@University of Nebraska - Lincoln, octubre de 2019. https://digitalcommons.unl.edu/senatedocs/2/.

[2] Serabian, Ryan y Lee Foster. "La campaña de influencia pro-PRC se expande a docenas de plataformas de redes sociales, sitios web y foros en al menos siete idiomas, intentó movilizar físicamente a los manifestantes en los EE. UU." Mandiant. Mandiant, 7 de septiembre de 2021. https://www.mandiant.com/resources/pro-prc-influence-campaign-expands-dozens-social-media-platforms-websites-and-forums.