COMUNICADO DE PRENSA

Diciembre 2024 ES

PERSPECTIVAS DEL ESTUDIO HISTÓRICO DE ATHENA SOBRE LA MANIPULACIÓN E INTERFERENCIA DE LA INFORMACIÓN EXTRANJERA

El consorcio ATHENA, formado por 14 socios de 11 países, ha respondido a la iniciativa European Democracy Shield. Sobre la base del análisis de 32 estudios de caso de manipulación e interferencia de información extranjera (FIMI) y el análisis de las tácticas, técnicas y procedimientos (TTP) utilizados por los atacantes, el consorcio proporcionó recomendaciones de política. Un informe histórico con El informe de ATHENA sobre las manifestaciones de FIMI tardó más de un año en la redacción, tiene 1.400 notas a pie de página, un indicador de los numerosos artículos, historias de periódicos, blogs, informes, discursos consultados por los socios, incluidas entrevistas en profundidad con más de 20 expertos que hacen contribuciones originales en la lucha europea contra FIMI.

Perspectivas clave

Adaptación a la evolución de las tácticas: vigilancia contra los actores del FMI

Los actores de FIMI utilizan una amplia gama de TTP y plataformas para evadir la detección y difundir sus mensajes. Los defensores necesitan una vigilancia y adaptación constante de las contramedidas para la evolucionan de las tácticas de los actores malintencionados.

- La variedad de estudios de casos indica una proliferación e inventiva de TTP empleados por los atacantes de FIMI. En consecuencia, la atribución es un desafío. Algunos atacantes cubren bien sus huellas o se involucran en la negación. El análisis FIMI requiere una comprensión de los diferentes tipos de atacantes en las campañas de desinformación, sus motivaciones y los TTP que utilizan. El consorcio ATHENA analizó casos de FIMI de Rusia, China, Corea del Norte, Turquía, Arabia Saudita, Irán e India, y encontró que Rusia está involucrada en FIMI más que cualquier otro país.

Aliados involuntarios de FIMI: el papel de los "idiotas útiles" en FIMI

El éxito de estas campañas a menudo depende de los "idiotas útiles", individuos que involuntariamente apoyan una causa o agenda, a menudo política o ideológica, sin comprender completamente sus implicaciones, particularmente cuando esa causa es manipuladora o dañina. La frase se utilizó para describir a los simpatizantes occidentales del comunismo soviético durante la Guerra Fría. El término se utiliza ahora de manera más amplia para describir a las personas que, en su entusiasmo o ingenuidad, apoyan movimientos, organizaciones o regímenes que, en última instancia, los manipulan o explotan.

Amplificar la desconfianza y debilitar las alianzas

Los atacantes emplean eficazmente técnicas de guerra de la información (como la distorsión del contenido y la explotación de las noticias de última hora) para amplificar la desconfianza dentro de la UE, debilitar las alianzas transatlánticas y promover políticos que simpatizan con sus causas.

- Varios actores de amenazas, incluidos grupos patrocinados por el estado, organizaciones criminales, hacktivistas e individuos con intenciones maliciosas, a veces trabajan juntos sin ningún acuerdo porque se adapta a sus objetivos compartidos, pero descoordinados. Explotando una infraestructura que les permite ocultar su identidad a través del anonimato, los atacantes de FIMI encuentran en las redes sociales un terreno fértil para cultivar y propagar su propaganda.

Aunque el FIMI se asocia frecuentemente con las elecciones, tiene un alcance mucho más amplio y sigue prosperando incluso después de las elecciones del Parlamento Europeo (PE) del 9 de junio de 2024. Sigue existiendo una amenaza creciente para la sociedad democrática. El impacto real de una campaña FIMI es incierto. La eficacia de estas campañas y el impacto de las contramedidas occidentales siguen siendo objeto de análisis y debate en curso.

Los estudios de caso de ATHENA mostraron que las redes sociales desempeñaron un papel clave en la distribución de desinformación, frecuentemente acompañada de hechos distorsionadores (53,3%) y aprovechando las narrativas existentes (50%). Esto refuerza el papel de **las redes sociales como conducto principal para la desinformación, diseñada para distorsionar los hechos, abrumar a los usuarios y reforzar el contenido engañoso.**

Una de las mejores defensas contra la desinformación es la transparencia, la comunicación efectiva y el uso de contranarrativas que desafíen la desinformación dirigida a la Unión Europea. Evaluar diferentes incidentes de desinformación implica ser autocrítico y tomarse en serio la relación de confianza entre las instituciones europeas y las sociedades de los diferentes Estados miembros.

La UE ha desarrollado diversas medidas para combatir la desinformación, incluida la Estrategia de Ciberseguridad de la UE[1] e iniciativas a través del Centro Europeo de Excelencia para la Lucha contra las Amenazas Híbridas[2].

---

[1] https://digital-strategy.ec.europa.eu/en/policies/cybersecurity-strategy
[2] https://www.hybridcoe.fi/

Recomendaciones

- Una contramedida multifacética contra la desinformación Las contramedidas eficaces contra las campañas de desinformación requieren un enfoque multifacético, que implique la cooperación entre los gobiernos, las redes sociales, la sociedad civil y el público. Sin embargo, este enfoque de toda la sociedad solo puede lograrse de manera realista si las partes interesadas que participan en la lucha contra el FIMI comparten un "lenguaje" común, como los marcos DISARM[3] y STIX[4], para armonizar el seguimiento, el análisis, la evaluación y la respuesta a las operaciones del FIMI.

Los gobiernos y las organizaciones de la sociedad civil (OSC) deben centrarse en iniciativas de alfabetización mediática para ayudar a los ciudadanos a evaluar críticamente las fuentes de noticias y evaluar la credibilidad y los motivos detrás de la información sobre ellas. **Se debe alentar a las personas a cuestionar la información en las campañas públicas.** En el caso de las medidas específicas adoptadas en respuesta a los ataques de FIMI, tanto los ciudadanos como los profesionales deben poder consultar fuentes oficiales o informes de instituciones de investigación creíbles, consorcios de proyectos y grupos de reflexión que se centren en la desinformación y la ciberseguridad.

Fomento de la verificación de datos Los Estados miembros de la UE deben promover las técnicas de verificación de datos de imágenes y vídeos para ayudar a las personas a identificar contenidos manipulados y otras formas de engaño digital. Educar a los ciudadanos, incluidos los niños en edad escolar, sobre las tácticas de FIMI puede ayudarlos a actuar como primera línea de defensa, reduciendo significativamente la difusión y el impacto de la información falsa.

- Equipo de respuesta rápida contra la desinformación Los gobiernos deberían establecer equipos de respuesta rápida capacitados para desacreditar la FIMI tan pronto como surja. Dichos equipos deberían estar integrados por funcionarios gubernamentales, académicos, organizaciones de la sociedad civil y periodistas especializados en la verificación de datos. Los gobiernos deben fortalecer los mecanismos de supervisión, mejorar la transparencia y colaborar más estrechamente con las organizaciones de verificación de datos para mitigar el impacto de la FIMI.

Inversiones urgentes en herramientas multilingües

El Servicio Europeo de Acción Exterior (SEAE), el servicio exterior de la UE, debe dar prioridad a la inversión en herramientas de seguimiento multilingües capaces de detectar FIMI en diferentes lenguas. Esto permitiría una identificación más rápida de contenidos manipuladores en diferentes contextos lingüísticos y regionales.

Intercambio de conocimientos

La CE debería fomentar los proyectos financiados por la UE que aborden el FIMI para establecer redes y compartir conocimientos con otros proyectos similares en los Estados miembros, Estados Unidos, Canadá, Australia, Japón, América Latina y otros países que se resisten a la manipulación de la información y la injerencia extranjeras.

Para obtener conclusiones y recomendaciones más detalladas de los estudios de caso, **consulte el documento informativo** al que también se puede acceder en el **sitio web de ATHENA**, donde puede obtener más información sobre el proyecto.

[3] https://disarmframework.herokuapp.com/
[4] https://oasis-open.github.io/cti-documentation/stix/intro.html

Consorcio

CONTACTO

Email: athena.comms@trilateralresearch.com

Funded by the European Union (grant number 101132686). UK participants in Horizon Europe Project ATHENA are supported by UKRI grant number 10107667 (Trilateral Research). Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or European Research Executive Agency (REA) or UKRI. Neither the European Union nor the granting authority nor UKRI can be held responsible for them. HORIZON-CL2-2023-DEMOCRACY-01.