ПРЕС РЕЛІЗ

Грудень 2024 УКР

ВИСНОВКИ ДОСЛІДЖЕННЯ ATHENA ПРО МАНІПУЛЯЦІЇ ТА ВТРУЧАННЯ ІНОЗЕМНОЇ ІНФОРМАЦІЇ

Консорціум ATHENA з 14 партнерів з 11 країн долучилися до ініціативи European Democracy Shield. Ґрунтуючись на аналізі **32 кейсів маніпулювання іноземною інформацією та втручання (FIMI)** та аналізу **тактики, методів і процедур (TTP),** що використовуються зловмисниками, консорціум надав відповідні рекомендації. Звіт з доповіддю ATHENA про прояви FIMI готувався більше року, складається з1400 виносок - показник численних статей, газетних історій, блогів, звітів, виступів, з якими консультувалися партнери, - включаючи інтерв'ю з більш ніж 20 експертами, які зробили безцінний внесок у європейську боротьбу проти FIMI.

Ключові висновки

Адаптація до мінливої тактики: пильність щодо суб'єктів ФМІ

Суб'єкти FIMI використовують широкий спектр TTP і платформ для ухилення від виявлення та поширення своїх повідомлень. Захисники потребують постійної пильності та адаптації контрзаходів у міру того, як еволюціонує тактика зловмисників.

- Спектр тематичних досліджень вказує на поширення та винахідливість TTP, які використовують зловмисники FIMI. Отже, атрибуція є складним завданням. Деякі зловмисники добре замітають сліди або вдаються до заперечення. Аналіз FIMI вимагає розуміння різних типів зловмисників у кампаніях з дезінформації, їхньої мотивації та TTP, які вони використовують. Консорціум ATHENA проаналізував випадки FIMI з Російської Федерації, Китаю, Північної Кореї, Туреччини, Саудівської Аравії, Ірану та Індії і виявив, що Росія бере участь у FIMI більше, ніж будь-яка інша країна.

Мимовільні союзники FIMI: роль «корисних ідіотів» у FIMI

Успіх цих кампаній часто залежить від «корисних ідіотів» – людей, які мимоволі підтримують справу чи порядок денний – часто політичний чи ідеологічний – не до кінця розуміючи їх наслідки, особливо коли ця справа є маніпулятивною або шкідливою. Цей вислів використовувався для опису західних симпатиків радянського комунізму під час холодної війни. Зараз цей термін використовується ширше для опису людей, які у своєму ентузіазмі чи наївності підтримують рухи, організації чи режими, які в кінцевому рахунку маніпулюють або експлуатують їх.

Посилення недовіри та ослаблення альянсів
Зловмисники ефективно використовують методи інформаційної війни (такі як спотворення контенту та використання екстрених новин), щоб посилити недовіру в ЄС, послабити трансатлантичні альянси та просувати політиків, які симпатизують їхнім справам.

- Різні суб'єкти загроз, включаючи спонсоровані державою групи, злочинні організації, хактивістів і осіб зі зловмисними намірами, іноді працюють разом без будь-яких домовленостей, оскільки це відповідає їхнім спільним, але неузгодженим цілям. Використовуючи методи, яка дозволяє їм зберігати анонімність, зловмисники FIMI знаходять у соціальних мережах необхідний ґрунт для культивування та поширення своєї пропаганди.

Незважаючи на те, що FIMI часто асоціюється з виборами, її охоплення є набагато ширшим і вона продовжує процвітати, як наприклад, після виборів до Європейського парламенту (ЄП) 9 червня 2024 року. Загроза демократичному суспільству залишається зростаючою. Фактичний вплив кампанії FIMI є невизначеним. Ефективність цих кампаній та вплив західних контрзаходів залишаються предметом постійного аналізу та дискусій.

Дослідження ATHENA показали, що соціальні мережі відіграють ключову роль у поширенні дезінформації, часто у поєднанні з викривленням фактів (53,3%) та використанням існуючих наративів (50%). Це посилює роль **соціальних мереж як основного каналу дезінформації, призначеної для спотворення фактів, перевантаження користувачів і підсилення контенту, що вводить в оману.**

Одним із найкращих засобів захисту від дезінформації є прозорість, ефективна комунікація та використання контрнаративів, які кидають виклик дезінформації, спрямованій проти політики Європейського Союзу. Оцінка різних інцидентів дезінформації передбачає самокритичність і серйозне ставлення до відносин довіри між європейськими інституціями та суспільствами різних держав-членів.

ЄС розробив різноманітні заходи для боротьби з дезінформацією, включаючи Стратегію кібербезпеки ЄС[1] та ініціативи через Європейський центр передового досвіду з протидії гібридним загрозам[2].

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

Рекомендації

- Всезагальна протидія дезінформації Ефективні заходи протидії дезінформаційним кампаніям вимагають багатогранного підходу, що включає співпрацю між урядами, соціальними мережами, громадянським суспільством та громадськістю. Однак такий загальносуспільний підхід може бути реалістично досягнутий лише за умови того, що зацікавлені сторони, які займаються протидією FIMI, спільними «мовами», такими як рамки DISARM[3] та STIX[4] , для гармонізації моніторингу, аналізу, оцінки та реагування на операції FIMI.

Розбудова критичного громадянського середовища
Уряди та організації громадянського суспільства (ОГС) повинні зосередитися на ініціативах з медіаграмотності, щоб допомогти громадянам критично оцінювати джерела новин та оцінювати достовірність і мотиви, що стоять за інформацією про них. **Окремих осіб слід заохочувати ставити під сумнів інформацію в публічних кампаніях.** Щодо конкретних дій, вжитих у відповідь на атаки FIMI, громадяни та практики повинні мати можливість звертатися до офіційних джерел або звітів надійних дослідницьких установ, проектних консорціумів та аналітичних центрів, які зосереджуються на дезінформації та кібербезпеці.

Сприяння фактчекінгу Держави-члени ЄС повинні розвивати навички перевірки фактів у зображеннях та відео, щоб допомогти людям виявляти маніпульований контент та інші форми цифрового обману. Ознайомлення громадян, у тому числі дітей шкільного віку, з тактикою FIMI може допомогти їм діяти як перша лінія захисту, значно зменшуючи поширення та вплив неправдивої інформації.

- Група швидкого реагування з дезінформації Уряди повинні створити групи швидкого реагування, навчені розвінчувати FIMI, як тільки вона з'являється. До таких команд мають увійти урядовці, науковці, громадські організації та журналісти, які перевіряють факти. Уряди повинні зміцнити механізми моніторингу, підвищити прозорість і тісніше співпрацювати з організаціями, що перевіряють факти, щоб пом'якшити вплив FIMI.

Термінові інвестиції в багатомовні інструменти
Європейська служба зовнішніх справ (EEAS), дипломатична служба ЄС, повинна приділяти першочергову увагу інвестиціям у багатомовні інструменти відстеження, здатні виявляти FIMI на різних мовах. Це дозволило б швидше ідентифікувати маніпулятивний контент у різних мовних та регіональних контекстах.

Обмін знаннями
Європейська Комісія повинна заохочувати фінансовані ЄС проекти, спрямовані на FIMI, налагоджувати зв'язки та обмінюватися знаннями з іншими подібними проектами в державах-членах, США, Канаді, Австралії, Японії, Латинській Америці та інших країнах, які протистоять іноземним інформаційним маніпуляціям та втручанню.

Більш детальні висновки та рекомендації з тематичних досліджень можна знайти в аналітичному документі, який також можна знайти на веб-сайті ATHENA, де ви можете дізнатися більше про проект.

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

Консорціум

Контакт

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.