COMMUNIQUÉ DE PRESSE

Décembre 2024 FR

APERÇU DE L'ÉTUDE PHARE D'ATHENA SUR LA MANIPULATION ET L'INGÉRENCE DE L'INFORMATION ÉTRANGÈRE

Le consortium ATHENA, composé de 14 partenaires venant de 11 pays, a répondu à l'initiative du Bouclier européen pour la démocratie. Se basant sur l'analyse de 32 études de cas de **manipulation et d'ingérence de l'information étrangère (FIMI) et de tactiques, techniques et procédures (TTP)** utilisées par les attaquants, le consortium a fourni des recommandations politiques. Le rapport réalisé dans le cadre du projet ATHENA sur les manifestations du FIMI a nécessité plus d'un an de rédaction. Il comporte 1 400 notes de bas de page - un indicateur des nombreux articles, articles de journaux, blogs, rapports, discours consultés par les partenaires - y compris des entretiens approfondis avec plus de 20 experts apportant des contributions originales à la lutte européenne contre le FIMI.

Principales informations

S'adapter à l'évolution des tactiques : une vigilance face aux acteurs des FIMI

Les auteurs de FIMI utilisent un large éventail de TTP et de plateformes pour échapper à la détection et diffuser leurs messages. Les défenseurs doivent faire preuve d'une vigilance constante et adapter leurs contre-mesures en fonction des tactiques des acteurs malveillants.

- L'éventail des études de cas indique une prolifération et une inventivité des TTP employés par les attaquants FIMI. Attribuer une action FIMI devient un véritable défi dans la mesure où certains attaquants brouillent bien leurs traces ou nient toute implication. L'analyse FIMI nécessite de comprendre les différents types de profils d'attaquants dans les campagnes de désinformation, leurs motivations et les TTP utilisés. Le consortium ATHENA a analysé les cas de FIMI venant de Russie, de Chine, de Corée du Nord, de Turquie, d'Arabie saoudite, d'Iran et d'Inde, et a constaté que la Russie s'engageait dans le processus plus que tout autre pays.

Alliés involontaires des FIMI: le rôle des « idiots utiles » dans le processus

Le succès de ces campagnes dépend souvent des « idiots utiles », des individus soutenant involontairement une cause ou un programme – souvent politique ou idéologique – sans en comprendre pleinement les implications, en particulier lorsque cette cause est manipulatrice ou nuisible. L'expression a été utilisée pour décrire les sympathisants occidentaux au communisme soviétique pendant la guerre froide. Le terme est considéré plus largement aujourd'hui pour décrire les personnes qui, par enthousiasme ou naïveté, soutiennent des mouvements, des organisations ou des régimes finissant par les manipuler ou les exploiter.

Amplifier la méfiance et affaiblir les alliances

Les attaquants emploient efficacement des techniques de guerre de l'information (telles que la distorsion du contenu et l'exploitation des événements d'actualité) pour amplifier la méfiance des citoyens au sein de l'UE, affaiblir les alliances transatlantiques et promouvoir des politiciens favorables à leurs causes.

- Divers acteurs de la menace, y compris des groupes parrainés par des États, des organisations criminelles, des hacktivistes et des individus mal intentionnés, travaillent parfois ensemble sans aucun accord car cela convient à leurs objectifs communs, mais de façon non coordonnée. Exploitant une infrastructure qui leur permet de dissimuler leur identité par l'anonymat, les attaquants de FIMI trouvent dans les réseaux sociaux un terrain fertile pour cultiver et faire proliférer leur propagande.

Bien que le concept de FIMI soit souvent associé aux élections, il a une portée beaucoup plus large et continue de prospérer même après les élections du Parlement européen (PE) du 9 juin 2024. La société démocratique demeure de plus en plus menacée. Les conséquences réelles des campagnes FIMI sont incertaines. L'efficacité de ces dernières et l'impact des contre-mesures occidentales restent des sujets d'analyse et de débat qui sont encore en cours à l'heure actuelle.

Les études de cas présents dans le rapport rédigé par le consortium ATHENA ont montré que les réseaux sociaux jouaient un rôle clé dans la diffusion de désinformation, souvent associés à des faits déformants (53,3 %) et à l'exploitation de récits existants (50 %). Cela renforce le rôle des **médias sociaux en tant que principal vecteur de désinformation, conçu pour déformer les faits, submerger les utilisateurs et renforcer le contenu trompeur.**

Parmi les meilleures défenses contre la désinformation figurent la transparence, une communication efficace et l'utilisation de contre-discours qui contestent la désinformation visant l'Union européenne (UE). L'évaluation des différents incidents de désinformation implique d'être autocritique et de prendre au sérieux la relation de confiance entre les institutions européennes et les sociétés des différents États membres.

L'UE a mis en place diverses mesures pour lutter contre la désinformation, notamment la stratégie de cybersécurité de l'UE[1] et des initiatives par l'intermédiaire du Centre d'excellence européen pour la lutte contre les menaces hybrides[2].

---

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

Recommandations

- Une contre-mesure multiforme contre la désinformation Les contre-mesures efficaces contre les campagnes de désinformation nécessitent une approche multidimensionnelle, impliquant une coopération entre les gouvernements, les médias sociaux, la société civile et le public. Cependant, cette approche pansociétale ne peut être réalisée de manière réaliste que si les parties prenantes engagées dans la lutte contre les FIMI partagent un « langage » commun tel que les cadres DISARM[3] et STIX[4] pour harmoniser le suivi, l'analyse, l'évaluation et la réponse aux opérations FIMI.

Les gouvernements et les organisations de la société civile (OSC) devraient se concentrer sur les initiatives d'éducation aux médias pour aider les citoyens à évaluer de manière critique les sources d'information et la crédibilité et les motivations qui les sous-tendent. **Les individus devraient être encouragés à remettre en question l'information dans les campagnes publiques.** Pour des actions spécifiques prises en réponse aux attaques FIMI, les citoyens et les praticiens devraient être en mesure de consulter des sources officielles ou des rapports institutionnels de recherche crédibles, de consortiums de projets et de groupes de réflexion qui se concentrent sur la désinformation et la cybersécurité.

Les États membres de l'UE devraient promouvoir les compétences en matière de vérification des faits, en utilisant des images et des vidéos afin d'aider les individus à identifier les contenus manipulés et d'autres formes de tromperie numérique. **Éduquer les citoyens, y compris les enfants en âge d'être scolarisés, sur les tactiques FIMI peut les aider à agir rapidement, réduisant considérablement la propagation et l'impact des fausses informations.**

- Les gouvernements devraient mettre en place des équipes d'intervention rapide formées pour désamorcer les FIMI dès qu'elles apparaissent. Ces équipes pourraient être composées de responsables gouvernementaux, d'universitaires, d'OSC et de journalistes chargés de vérifier les faits. Les gouvernements devraient renforcer les mécanismes de surveillance, améliorer la transparence et travailler plus étroitement avec les organisations de vérification des faits pour atténuer l'impact des FIMI.

Le Service européen pour l'action extérieure (SEAE), devrait privilégier les investissements dans des outils de suivi multilingues capables de détecter les FIMI dans différentes langues. Cela permettrait d'identifier plus rapidement les contenus manipulateurs dans différents contextes linguistiques et régionaux.

La Commission européenne devrait encourager les projets financés par l'UE concernant les FIMI à se mettre en réseau et à partager leurs connaissances avec d'autres projets similaires dans les États membres, mais également aux États-Unis, au Canada, en Australie, au Japon, en Amérique latine et dans d'autres pays qui résistent à la manipulation et à l'ingérence de l'information étrangère.

Si vous souhaitez avoir accès aux conclusions et recommandations plus détaillées des études de cas, consultez le document d'information sur le site internet **d'ATHENA Website**, où vous pouvez en savoir plus sur le projet.

---

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

Consortium

CONTACT

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.