Remarques sur la question de la manipulation de l'information dans le rapport ENISA2023

Anaïs Meunier

22 octobre 2023

Il y a quelques jours, le rapport de l'ENISA sur le panorama de la menace était diffusé, celui-ci, très complet traite des menaces cyber en général et un chapitre est consacré aux manipulations de l'information.

Le document prend le temps de redéfinir les termes "manipulations de l'information" et de les situer dans le contexte de la menace cyber. Ainsi, les FIMI : *Foreign Information Manipulation and Interference (FIMI) describes a mostly non-illegal pattern of behaviour that threatens or has the potential to negatively impact values, procedures and political processes. Such activity is manipulative in character, conducted in an intentional and coordinated manner. Those who undertake such activity may be state or non-state actors, including their proxies inside and outside their own territory798. The current chapter focuses on information manipulation and interference regardless of its origin.* Cette volonté de clarifier les concepts est essentielle, j'y accorde beaucoup d'importance, bien que, comme tout cadre conceptuel et opérationnel, il présente des limites.

Dans le chapitre consacré aux manipulations de l'information, l'ENISA (l'Agence de l'Union européenne pour la cybersécurité) met l'accent sur le comportement de l'attaquant plutôt que sur les récits exploités.C'est un élément crucial qui contribue à rétablir de l'objectivité dans le débat, car il ne se positionne pas sur la question de la vérité, ce qui demeure un enjeu fondamental dans une société démocratique, mais sur celui de l'intentionalité. Ainsi, se fonder sur le comportement permet de mettre en lumière l'intention malveillante de l'attaquant et d'intégrer le champ des *Foreign Information Manipulation and Interference* (FIMI, ce que nous appellerions en français : ingérences numériques étrangères) dans le domaine de la cybersécurité.

Cela revêt une importance particulière pour l'agence, car l'un des piliers de la cybersécurité est de garantir la sécurité des systèmes d'information, et les FIMI vont à l'encontre de cette garantie. Enfin, les deux types d'attaques se manifestent au sein de campagnes hybrides, comme le souligne notamment le corpus analysé dans le rapport de l'ENISA, qui repose sur des données issues de la veille du SEAE. Il est donc essentiel d'étudier et de combattre dans les différents domaines d'un même champ.

Le rapport de l'ENISA sur le paysage de la menace repose sur les observations du SEAE. Il débute en mettant en avant les tactiques les plus exploitées, telles qu'elles sont décrites dans la matrice Disarm.

Deux remarques principales peuvent être formulées En premier lieu, il est essentiel de souligner que toutes les tactiques ne sont pas équivalentes dans la matrice DISARM. Bien que

DISARM se fonde sur le travail du MITRE ATT&CK pour décrire de manière dynamique le comportement de l'attaquant, les phases qui se situent dans le *"Left of Boom"* (avant l'explosion de la campagne) et le *"Right of Boom"* n'ont pas exactement le même statut. En général, les éléments du *Left* sont déduits, car il est difficile de déterminer quand l'attaquant prépare sa campagne, tente de recruter des influenceurs ou fait appel à une ferme de *bots*. En fonction des méthodologies utilisées, ces éléments seront plus ou moins présents dans la description de la campagne. L'analyste doit donc décider s'il doit ou non inclure des techniques, tactiques et procédures (TTPs) qu'il ne peut que déduire de ses observations et non pas observer directement.

Deuxième limite, le corpus fait remonter de nombreux incidents liés au conflit russo-ukrainien. Cette observation est pertinente car c'est dans ce contexte que l'on observe le plus grand nombre de campagnes ou d'incidents hybrides. Cependant, cela ne représente pas la totalité du paysage des attaques informationnelles en Europe. Au-delà de ces deux éléments, le chapitre sur les FIMI et les campagnes et incidents hybrides révèle des points très intéressants :

— les campagnes n'ont pas besoin d'être très sophistiquées pour être efficaces. Leur persistance est la caractéristique la plus déterminante. Les TTPs les plus couramment exploitées incluent l'utilisation de faux comptes, la création de sites web inauthentiques, l'exploitation de médias d'État, ainsi que l'utilisation de boucles de rétroaction sur les réseaux sociaux et les médias traditionnels (ce qui s'avère particulièrement efficace).
— l'utilisation de l'intelligence artificielle permet de créer des contrefaçons de qualité à moindre coût (grâce à l'accessibilité et à la facilité d'utilisation des outils d'IA générative).
— Bien que le public soit parfaitement capable de discerner ce qui relève de la contrefaçon et de mettre en place des mécanismes de défense, l'usage massif de cette technique, qui permet d'agir rapidement, à grande échelle et avec un volume important, rend l'utilisation de l'IA dangereuse (voir figure 45 page 119).

Enfin, l'un des derniers points pertinents soulevés concerne l'externalisation de plus en plus fréquente, que ce soit pour offrir des services de désinformation (Disinformation-as-a-Service) ou pour proposer des services de désinformation à la demande (Disinformation-for-Hire). Cette tendance est très présente dans le domaine de la cybercriminalité et est mise en avant dans le dernier rapport sur la menace de l'ANSSI. L'ENISA cite notamment le travail d'enquête réalisé sur la Team Jorge comme exemple significatif. Cette externalisation nourrit en un écosystème qui repose sur la publicité.
L'utilisation de la publicité pour générer des revenus grâce à la désinformation est sans doute le point central qui permet d'alimenter cette économie souterraine.