



L'intelligence artificielle (IA), entre menaces et opportunités

Publié le 06 Mai 2024

Temps de lecture : 4 min



Si les concepts de l'intelligence artificielle datent des années 50 et qu'elle est intégrée dans de nombreuses solutions depuis maintenant plusieurs dizaines d'années, l'année 2023 aura été marquée pour le grand public par la découverte de l'intelligence artificielle générative et notamment celles basées sur les grands modèles de langage.

L'IA, une opportunité pour les cybercriminels ?

Compréhension du langage naturel, traduction, production de contenus texte, vidéo ou audio, traitement massif de données, automatisation et résolution de problèmes complexes... Les capacités et l'accessibilité de ces nouveaux modèles d'intelligence

artificielle peuvent à la fois émerveiller comme effrayer, tant le champ des possibles semble étendu.

Bien évidemment, **comme toute évolution technologique, les possibilités offertes par l'intelligence artificielle ne peuvent que retenir l'attention des cybercriminels.** Des modèles d'IA générative cybercriminels n'ont d'ailleurs pas tardé à être développés et rendus disponibles (WormGPT, FraudGPT, ThreatGPT...).

En l'état des connaissances encore balbutiantes sur le sujet et au-delà de toute spéculation, **cela ne voudrait toutefois pas pour autant annoncer un bouleversement du panorama des cybermenaces.** En effet, si l'intelligence artificielle peut améliorer la productivité des cybercriminels et la sophistication de leurs modes opératoires, ceux-ci resteront sans doute, du moins encore un temps, très similaires dans leurs principes.

Depuis plusieurs années, la cybercriminalité est devenue de plus en plus facilement accessible à de nouveaux acteurs disposant de faibles compétences techniques, au travers de services spécialisés commercialisés en ligne, notamment sur l'Internet sombre (darknet). L'arrivée de l'intelligence artificielle dans ces services ne peut qu'accroître cette tendance. **Le développement de l'utilisation de l'IA à des fins cybercriminelles et l'augmentation du nombre d'acteurs malveillants qui pourra en découler seront très probablement de nature à voir encore s'amplifier le nombre attaques et leur niveau d'élaboration.**

Quelles sont les cybermalveillances liées à l'IA ?

Aucun cas de malveillance pouvant être formellement imputé à l'intelligence artificielle n'a pu être recensé jusqu'à présent par [Cybermalveillance.gouv.fr](https://cybermalveillance.gouv.fr) sur son périmètre. Cette imputation restera toutefois souvent difficile à déterminer. En effet, si on peut toujours affirmer qu'un message, une publication ou un programme sont malveillants, il est souvent beaucoup plus délicat de déterminer avec certitude qu'ils ont pu être réalisés par, ou à l'aide, d'une intelligence artificielle.

Plusieurs faits d'utilisation malveillante de l'IA ont toutefois commencé à être rapportés à l'international dans des hypertrucages (*deepfakes*) audio, vidéo ou photo visant à détourner l'image de célébrités à des fins d'escroquerie, ou de personnalités politiques à des fins de manipulation de l'opinion, ou encore de cyberharcèlement à caractère pornographique...

En conclusion

Face au champ des possibles cybermalveillances liées à l'IA il convient donc d'aiguiser encore davantage son sens critique pour arriver à distinguer le vrai du faux.

Mais si l'intelligence artificielle peut constituer une menace dans son utilisation par les cybercriminels, elle s'imposera certainement aussi comme une opportunité d'aider les publics à mieux et plus facilement identifier les menaces et s'en protéger.

Pour aller plus loin

- Découvrez les principales tendances de la menaces et les chiffres clés de la plateforme Cybermalveillance.gouv.fr en 2023 dans notre [dernier rapport d'activité](#)

INSCRIVEZ-VOUS À LA NEWSLETTER

Tenez-vous informé(e) de l'actualité de la cybermalveillance et des nouvelles menaces



OK



À PROPOS

Qui sommes-nous ?

Presse

DIVERS

[Plan du site](#)

[Mentions légales](#)

[Politique de confidentialité](#)

[Accessibilité](#)

NOUS SUIVRE



[GOUVERNEMENT.FR](#) 

[LEGIFRANCE](#) 

[ELYSEE.FR](#) 

[FRANCE.FR](#) 

[SERVICE PUBLIC](#) 

[DATA.GOUV.FR](#) 