

## Veille technologique – Cybersécurité & Nouvelles technologies

Pour ma veille, j'ai utilisé Perplexity AI, une IA connectée au web qui me résume l'actualité. Grâce à une automatisation sur mon téléphone, je reçois deux fois par semaine (lundi et vendredi) un point sur l'actualité de la cybersécurité.

### Dis moi les actualités dans le domaine de la cybersécurité



Réponse



Sources 12

1 tâche ↗

En 2025, la cybersécurité est marquée par une forte augmentation et une sophistication accrue des attaques. Les ransomwares et les attaques par hameçonnage explosent, avec une multiplication par près de trois des attaques de ransomwares et une hausse spectaculaire des tentatives de compromission de mots de passe, qui atteignent désormais sept mille attaques par seconde chez certains grands fournisseurs comme Microsoft <sup>4 6</sup>. Les cybercriminels utilisent de plus en plus l'intelligence artificielle pour automatiser leurs attaques, générer des campagnes de phishing très crédibles et cibler les failles humaines au sein des organisations <sup>6 7 18</sup>.

Les attaques sur la chaîne d'approvisionnement et les objets connectés (IoT) sont en forte hausse, car ces points d'entrée restent souvent mal sécurisés et offrent des accès privilégiés aux réseaux d'entreprise <sup>7 9 18</sup>. La généralisation de la 5G élargit encore la surface d'attaque, rendant la sécurisation des réseaux et des appareils connectés cruciale <sup>9</sup>.

L'intelligence artificielle devient à la fois un outil d'attaque et de défense : elle permet aux attaquants d'automatiser et de personnaliser leurs offensives, mais elle aide aussi les défenseurs à détecter plus rapidement les menaces et à réagir en temps réel <sup>7 18 12</sup>. Face à cette évolution, les entreprises adoptent massivement des stratégies de « Zero Trust », où aucun utilisateur ou appareil n'est considéré comme fiable par défaut, et renforcent la sécurité du cloud pour protéger les données sensibles <sup>18 12</sup>.

Enfin, la menace des groupes étatiques ou d'hacktivistes organisés s'intensifie, notamment contre les infrastructures critiques comme l'énergie ou la finance, faisant de la cybersécurité un enjeu central de souveraineté et de résilience nationale <sup>6 7</sup>. Les autorités, comme l'ANSSI en France, publient de nouveaux plans stratégiques pour coordonner la réponse à ces menaces et encourager le développement des compétences en cybersécurité <sup>4</sup>.

voici un exemple de réponse que me renvoie perplexity, on peut voir que je peux consulter les sources utilisé pour produire cette réponse

---

## IA & Cybersécurité : une arme à double tranchant

Côté attaques :

- Phishing amélioré par IA

- Création de malwares polymorphes
- Génération de deep fakes (voix, vidéos)

Côté défense :

- Détection de comportements anormaux
- Réponse automatisée aux incidents (ex : blocage IP)
- Systèmes adaptatifs qui apprennent des attaques passées

L'IA est aussi très utile pour analyser les logs et le trafic réseau en temps réel.

---

## **Informatique quantique : un risque pour le chiffrement**

Quand elle sera suffisamment puissante, l'informatique quantique pourra casser les systèmes de chiffrement actuels.

Cela menace :

- Les transactions bancaires
  - Les certificats numériques
  - Les communications sécurisées (TLS/SSL)
- 

## **Les réponses aux menaces quantiques**

Cryptographie post-quantique :

Des algorithmes conçus pour résister aux attaques quantiques :

- CRYSTALS-Kyber. C'est un algorithme de chiffrement post-quantique qui permet à deux parties d'échanger une clé secrète de façon sécurisée, Il repose sur des mathématiques complexes appelées réseaux euclidiens
- Classic McEliece. Cet algorithme se base sur des codes correcteurs d'erreurs, une technique mathématique éprouvée depuis des décennies. Même si ses clés publiques sont assez grandes, il offre une très bonne sécurité et une grande rapidité de déchiffrement

- Rainbow. C'est un algorithme de signature post-quantique basé sur des équations polynomiales multivariées, un domaine mathématique difficile à inverser, même pour un ordinateur quantique. Il a finalement été écarté du processus de standardisation à cause de vulnérabilités découvertes, notamment des attaques permettant de récupérer la clé privée.
- SPHINCS+. C'est un algorithme de signature post-quantique basé sur des fonctions de hachage. Contrairement à d'autres algorithmes, il n'utilise pas de structures mathématiques complexes, ce qui le rend plus simple à analyser.

Cryptographie quantique (QKD) :

- Utilise les lois de la physique quantique pour sécuriser l'échange de clés de chiffrement. Son principe repose sur le fait que toute tentative d'interception modifie l'état des particules utilisées (comme des photons), ce qui rend toute attaque détectable.
- Le problème est que cette méthode reste coûteuse et difficile à déployer

---

## Conclusion

L'IA et l'informatique quantique sont en train de transformer la cybersécurité.

Il est donc essentiel de suivre ces évolutions pour anticiper les menaces et adapter les méthodes de protection.